UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA DE TELECOMUNICACIÓN

SISTEMAS DE TELECOMUNICACIÓN

PROYECTO FINAL DE CARRERA

DISEÑO E IMPLANTACION DE UN ENTORNO DE PRUEBAS PARA NATBOX

AUTORA: SARA MUÑOZ HURTADO

TUTOR: JOSE IGNACIO MORENO NOVELLA

Leganés, Febrero de 2014

Título: Diseño e Implantación de un entorno de pruebas para Natbox

Autor: Sara Muñoz Hurtado

Director: José Ignacio Moreno

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

AGRADECIMIENTOS

En primer lugar me gustaría agradecer a Mª Carmen y Rubén, las dos personas más importantes en mi vida, todo el apoyo que me han transmitido durante todos estos años de esfuerzo en los que han surgido sensaciones de todos los colores. Sabéis que sin vosotros no habría conseguido superarme.

Por supuesto, al profesor José Ignacio Moreno por sus consejos, paciencia y comprensión durante todo este proceso. Gracias.

Agradecer también a todos los compañeros que he conocido estos años entre las paredes de cada uno de los edificios de la UC3M y que sin saberlo, forman parte de mi crecimiento personal.

A ti también, para que seas consciente de lo que has conseguido y porque te mereces agradecértelo.

Finalmente, agradecer a esa persona que hace que cada día supere el anterior y que convierte la vida en una piñata de cumpleaños, todo el apoyo diario que me ha ayudado a poner fin a esta etapa de mi vida. Gracias Marta.

A todos, GRACIAS

RESUMEN

Actualmente el número de usuarios que dispone de dispositivos *always on,* ha incrementado en los últimos años gracias a la adaptabilidad demandada para poder responder a sus necesidades. Sin embargo, este hecho ha provocado un descenso en la disponibilidad de direcciones de Internet (IPv4) de los proveedores del servicio, quiénes deben implementar una solución transitoria hasta que se establezca el nuevo modelo de direccionamiento basado en el protocolo IPv6. En este proyecto, se muestra cómo a través de una de las técnicas de traducción de direcciones, NAT44 en este caso, podemos ofrecer acceso a los servicios demandados por parte de los usuarios de una operadora móvil resolviendo por el momento el problema de la escasez de direcciones públicas de Internet.

ABSTRACT

Nowadays the number of users who have "*always on"* devices has increased in the past few years thanks to the resilience required in order to meet their needs. Nevertheless, this fact has caused an Internet addresses availability decrease of the service providers, who should implement a temporary solution before a new routing protocol (IPv6) is established. This project demonstrates how we can provide demanded mobile operator services throughout one of address translation technique as NAT44, so the shortage problem of public Internet addresses is briefly solved.

INDICE GENERAL

INDICE FIGURAS

INDICE TABLAS

1 INTRODUCCION

1.1 Introducción del proyecto

El impacto que ha supuesto tanto Internet como sus aplicaciones en los sistemas de información han provocado un cambio en los hábitos de la sociedad forzando una transformación en el mercado de las telecomunicaciones, de sus modelos y conceptos originales.

Inicialmente los servicios móviles permitieron la posibilidad de comunicarse vía telefónica desde cualquier lugar. Posteriormente seguida de una revolución de las telecomunicaciones, los avances tecnológicos y la estandarización de ciertos sistemas facilitaron la creación de nuevos servicios que ensalzaron las redes móviles. Algunos de estos servicios como el buzón de voz, el envío y recepción de mensajes de texto… y su personalización, hicieron comprensible la penetración de los mismos en los últimos años.

Actualmente servicios basados en protocolos WAP, TCP, *Streaming*, P2P… han cumplido con el requisito de la sociedad de combinar servicios proporcionados por redes de datos, junto con las posibilidades que ofrecen los dispositivos móviles.

Gracias a analistas investigadores en IMS (International Protocol Multimedia System), hemos podido saber que el mercado en telefonía móvil inteligente experimentará un crecimiento muy pronunciado en los próximos años. Esta expansión se ve reforzada por el precio cada vez más asequible de los teléfonos y su adaptación a la necesidad de los consumidores.

El aumento de consumidores que poseen teléfonos y dispositivos con filosofía "*always on*" (*smartphones*, *tablets*, TV, elementos domésticos…) tiene como resultado un incremento en la demanda de direcciones de Internet. Como consecuencia, se presenta una relación inversamente proporcional entre esas peticiones y el número de direcciones IPv4 que poseen los proveedores del servicio de Internet, como ocurre en el caso de una operadora móvil.

1.2 Motivación

Las operadoras móviles deben adaptar por lo tanto su arquitectura a la evolución de las nuevas tecnologías para poder enfrentar el creciente número de peticiones de acceso a Internet. Además a esta situación se adhiere el problema del agotamiento de direcciones públicas Ipv4.

La única solución que resolvería totalmente este conflicto, está basada en la migración de las antiguas direcciones IPv4 a un nuevo protocolo IPv6 cuyo direccionamiento de red sería casi infinito.

Desafortunadamente, este proceso de migración no debe realizarse radicalmente pues existirían problemas de interoperabilidad con las direcciones IPv4. Deben modificarse las asignaciones tanto en la red que ofrece el servicio como la que lo contiene. Incluso este nuevo protocolo mantiene un crecimiento de desarrollo muy lento por lo que es necesario implementar sistemas que permitan la supervivencia del protocolo IPv4 hasta que se realice la migración total del nuevo sistema. Sin embargo, esta decisión se aplica a corto-medio plazo hasta que se extienda mayoritariamente el entorno IPv6 en los dispositivos y aplicaciones.

Es por ello que surge la necesidad de implementar la tecnología NAT44 que disminuye el agotamiento de direcciones públicas a través de las cuales se accede a Internet. Su función principal es ejercer de traductor entre las redes de datos por las que se transporta la información generada según los protocolos sobre los que se soportan los servicios demandados por los usuarios.

La idea es asignar unas direcciones privadas a los usuarios que demandan el acceso a Internet y compartirlas con el resto de usuarios que realicen otras peticiones. La gestión de esas peticiones se lleva a cabo por los distintos equipos que forman la red. Este plan de direccionamiento organiza un conjunto de direcciones IP para facilitar y simplificar la topología de la red para economizar estas direcciones.

1.3 Objetivos

Para comprobar si la tecnología NAT44 es una buena solución para disuadir la escasez de direcciones IPv4 públicas que impediría a los usuarios de una operadora móvil el acceso a Internet, **se analiza el comportamiento del acceso a los servicios de Internet entre la plataforma de NAT44 y la salida a la red pública, a través de la definición y síntesis de una batería de pruebas en un entorno controlado.**

Inicialmente, validamos el equipo elegido para llevar a cabo esa función, siguiendo unos criterios técnicos y de diseño previamente definidos.

Seguidamente sintetizamos el piloto de pruebas sobre el que realizaremos las pruebas específicas y cuyos resultados ayudarán a modificar en el caso de que fuera necesaria la arquitectura real que establece el sistema real de comunicaciones móviles.

Finalmente y siendo este el objetivo principal de este proyecto, se analiza el conjunto de pruebas definidas que muestran el comportamiento de algunos de los servicios más demandados en la red móvil.

Comprobaremos que el usuario puede acceder a los servicios deseados gracias a la implementación de la plataforma NAT44 y el desarrollo del mecanismo basado en pasarelas a nivel de aplicación. A través de una herramienta analizadora de protocolos, observaremos que el envío de paquetes entre la plataforma NAT44 y la salida a Internet es correcto.

1.4 Contenido de la Memoria

La memoria del proyecto se estructura de manera bien diferenciada en varios puntos:

En la primera parte se explica la problemática y necesidad del proyecto. **Cap1**

Posteriormente revisaremos la evolución de la red y los protocolos en los que se han basado el funcionamiento del equipo NAT44 para poder llevar a cabo las pruebas determinadas. **Cap2**

A continuación presentamos el escenario y las pruebas que muestran el desarrollo del proyecto. **Cap3**

El siguiente punto muestra los resultados obtenidos del capítulo anterior, así como las conclusiones y trabajos futuros extraídos después de la realización de las pruebas.**Cap4**

Seguidamente encontramos el presupuesto y diagrama de Gantt previsto para el desarrollo del proyecto. **Cap5**

Por último constan varios anexos: un glosario de términos necesario para comprender ciertos significados y una bibliografía dónde encontrar las referencias indicadas durante la memoria del proyecto.

2 ESTADO DEL ARTE

En este capítulo se introducen ciertos conceptos relacionados con la evolución que han sufrido las arquitecturas de las redes móviles como resultado de la demanda de nuevos servicios de red por parte de los usuarios. Además, continuando con este hecho, describiremos protocolos y mecanismos que permiten el acceso a la red pública y las técnicas que permiten el desarrollo de su interoperabilidad.

2.1 Evolución Redes Móviles

Para comprender la necesidad del proyecto es importante revisar la evolución que ha existido en las comunicaciones móviles en los últimos 20 años.

Puntualizando las claves de las cuatro Generaciones de Telefonía Móvil que se han vivido hasta el momento, comprobamos que la tendencia consiste en conseguir una convergencia global en una red única. El reflejo de esta idea se proyecta en la creación de nuevos servicios de movilidad así como de nuevas aplicaciones que permitan conciliar el nuevo desarrollo de la movilidad con el acelerado cambio de las tecnologías en los sistemas de comunicaciones

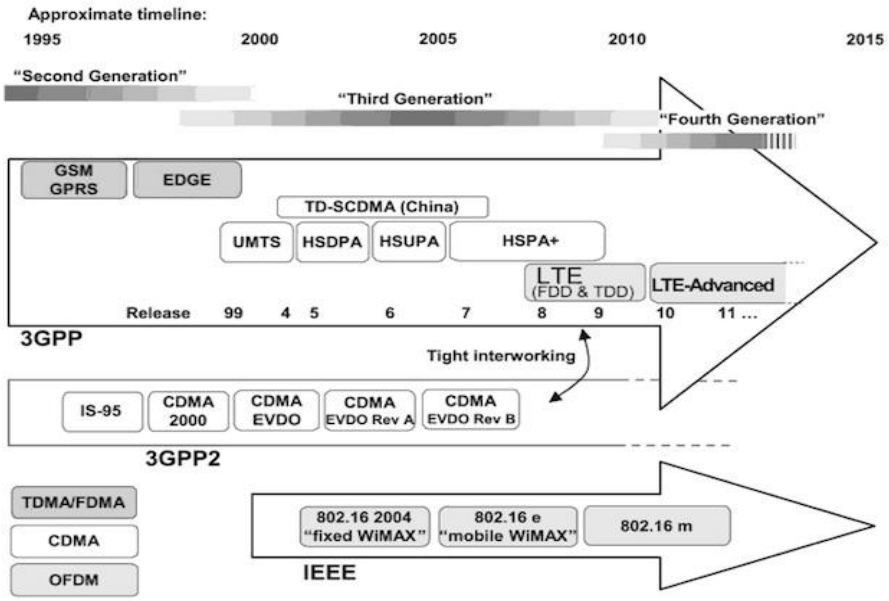


Figura 1: Evolución Tecnologías Redes Móviles

En la década de los **80** surge la Primera Generación de redes móviles o **1G**, cuyo escenario cuenta con una gran cantidad de sistemas incompatibles entre sí. La interfaz radio utilizada es analógica (**TMA**) y la multiplexión de frecuencia, separando 45MHz para transmisión (MS→BTS) y recepción (BTS→MS).

Al principio de los **90**, se introducen los sistemas digitales así como el despliegue de la tecnología **GSM**. De esta forma surge la Segunda Generación (**2G**), que utiliza una modulación digital, optimiza el espectro del que dispone y facilita la interconexión con la red tradicional **RDSI**. La transmisión de datos inalámbrica se basa en un canal dedicado a **velocidad máxima de 9.6Kbps**. Es decir, asignamos un canal de comunicación al usuario aunque no lo use. Se mejora la calidad de transmisión, se ofrecen servicios adicionales como **SMS** y la posibilidad de hacer "***roaming***", éxito más evidente del estándar.

Se muestra en la siguiente figura, la arquitectura de una red GSM basada en la conmutación de circuitos y que ofrece principalmente el servicio de voz. Se muestran los equipos necesarios para su funcionamiento. [1]

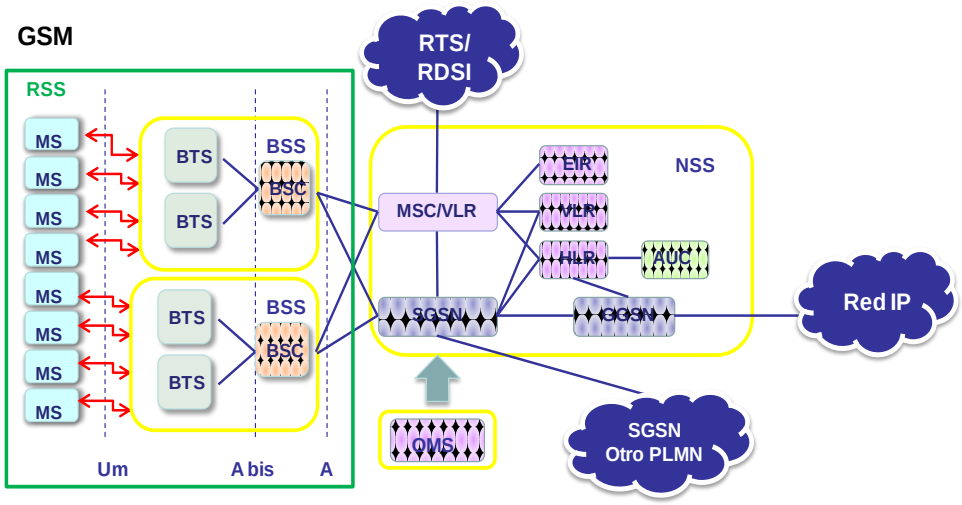


Figura 2: Arquitectura Red Móvil GSM

La siguiente fase de esta evolución conocida como **2.5G** surge a finales de esta década. A través del estándar **GPRS** se diseña esta red para transferir paquetes utilizando la interfaz de radio de GSM. Así se acopla a ese sistema una red de transporte, también conocida como (**IP *Backbone*)**, que paralelamente y utilizando los intervalos de tiempo libre cursa un tráfico que proviene de la **conmutación de paquetes** y las conexiones a **Internet.**

En este caso los canales son compartidos de forma dinámica, la asignación se aplica en caso de que exista una transmisión real de datos. Los usuarios pueden enviar datos con imágenes con una calidad de servicio "*best effort*", aquella que en ese momento pueda asignarse a cada uno.

La red **EDGE** que se presenta en la siguiente figura es un ejemplo de arquitectura basada en el nacimiento de la conmutación de paquetes y datos, y por lo tanto es el origen de la tecnología que permite la aparición de los ***smartphones***.

GPRS

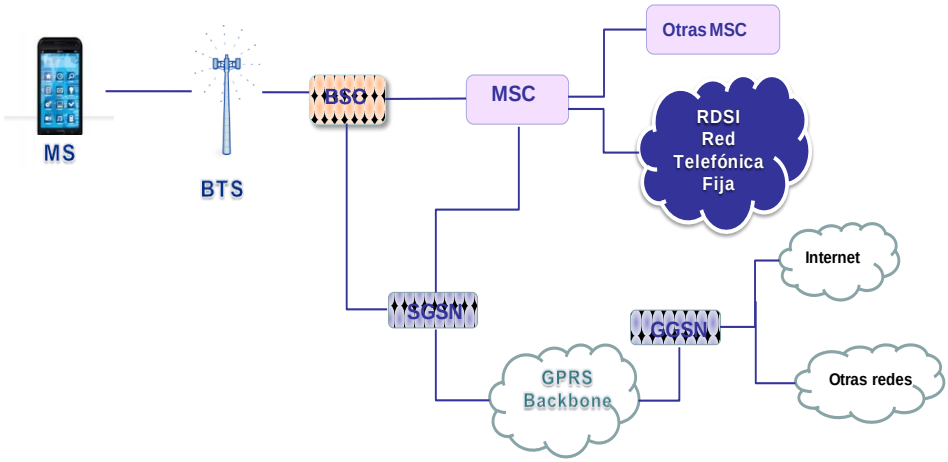


Figura 3: Arquitectura Red Móvil GPRS

En el año **2000** comienza la que sería una revolución de las comunicaciones en telefonía móvil. La generación de transmisión de voz y datos a través de telefonía móvil (**3G** o **UMTS**) se ralentizó más de lo esperado. Más allá de una adaptación de la tecnología anterior, era necesaria una **nueva infraestructura** que permitiera la **transmisión de datos en equipos, teléfonos móviles y espectro de frecuencias distintos** a todo lo conocido. Para el diseño de esta nueva arquitectura que cumple con el estándar UMTS, la organización **3GPP** ha establecido varias capas de funcionamiento.

Capa Servicios: despliegue rápido y centralizado de servicios.

Capa de Control: capacidad de red dinámica.

Capa conectividad: uso de cualquier tecnología de transmisión y tráfico de voz mediante **ATM/IP**.

A pesar de que esta tecnología fue introducida con mucho éxito y que es ideal en cuanto a servicios multimedia móviles se refiere (velocidades de transmisión superiores a los **3Mbps**), cuestiones como la **incapacidad para soportar múltiples sistemas de acceso radio** o **la ineficiencia en el mantenimiento de los dominios de circuitos y paquetes**, crean la necesidad de una nueva generación. [3]

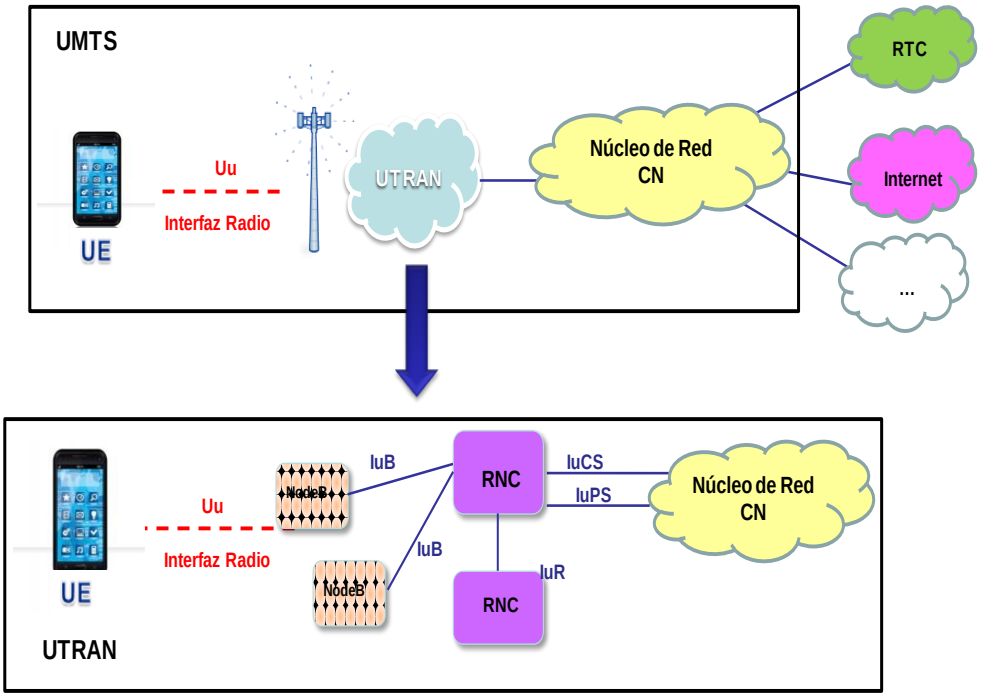


Figura 4: Arquitecturas Tecnología UMTS y Tecnología UTRAN

Actualmente la generación de telefonía móvil que se está desplegando, conocida como **LTE** o **4G**, está orientada a la convergencia entre redes de cables e inalámbricas fusionando tecnologías y protocolos. Consiste en un sistema basado en el **protocolo IP**, que mejora el uso de los recursos radioeléctricos. Algunas de las mejoras que propone este sistema son: velocidades de acceso superiores a los **100Mbps en movimiento y 1Gbps en reposo** con determinados **QoS**, así como la separación del plano de usuario y el plano de control a través de interfaces abiertas. Para el desarrollo de esta nueva tecnología la infraestructura radio del sistema ha cambiado por completo dando lugar al sistema **E-UTRAN**, que reduce el coste del nodo de control.

Las funciones del mismo han sido integradas junto con las de movilidad, calidad y recurso radio, en un nuevo nodo conocido como **eNB**. El principal problema de este sistema es la normalización de la voz en redes *All*-IP, ya que resulta muy complicado relacionar las redes tradicionales con LTE. Para solventar este problema surge **IMS**, una arquitectura global, con acceso independiente, basada en conectividad IP que proporciona tanto servicios multimedia como la comunicación básica de voz. [4]

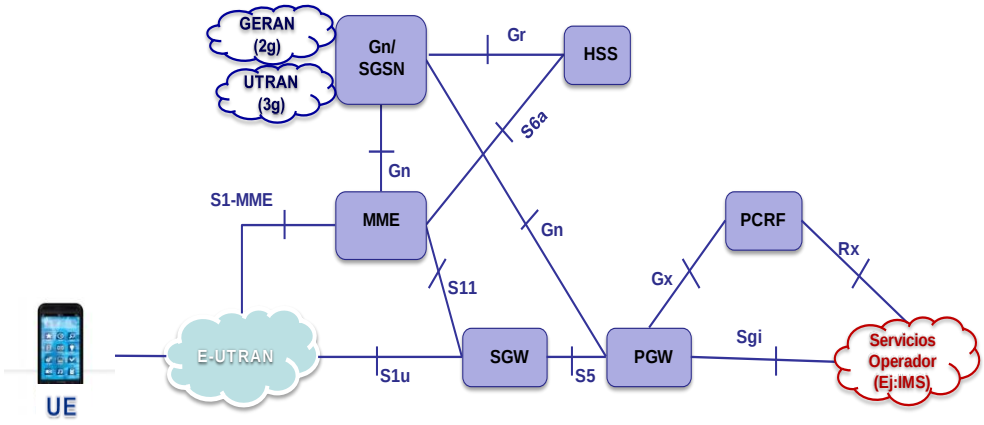


Figura 5: Arquitectura Red Móvil LTE

Para concluir con el repaso a la evolución de las generaciones móviles es relevante señalar que la tendencia consiste en conseguir movilidad sobre una única red, con dispositivos más funcionales y de menor tamaño que los ordenadores que surgieron hace 30 años.

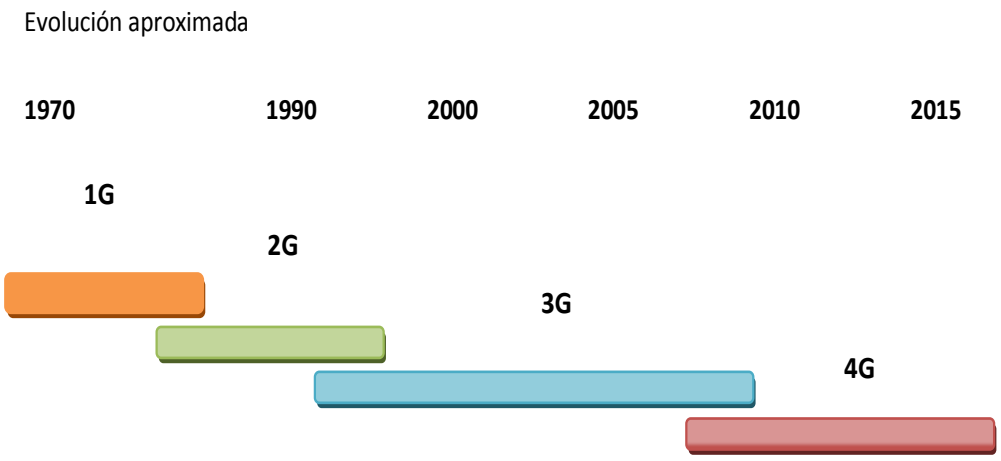


Figura 6: Evolución Generaciones Móviles

El impulso de LTE complicará la escasez de direcciones IPv4 puesto que la idea es asignar una dirección por dispositivo que quiera acceder a la red de 4G.

El aumento del tráfico de servicios de datos en las operadoras móviles aumenta progresivamente, especialmente con la implantación de *smartphones* y el desarrollo de nuevos servicios la mayor parte de banda ancha. Para afrontar la problemática del agotamiento de direcciones IP públicas disponibles para asignarlas a esos servicios.

2.2 Evolución Smartphones

Desde hace varios años hemos comprobado cómo Internet ha experimentado un asombroso crecimiento en los últimos años. En sus orígenes era una pequeña red compartida por sus creadores y actualmente mantiene conectados a todo el mundo. Este crecimiento se ha basado principalmente en la capacidad de generar servicios que los usuarios demandaban.

Es importante indicar que la mayor parte de la exigencia de estos servicios ha surgido en el entorno móvil. Por lo tanto se ha incrementado la necesidad de emplear unos dispositivos que pudieran soportar estos nuevos requerimientos. Hemos evolucionado en escasos años del teléfono que ofrecía el servicio básico de comunicación verbal o mensajería instantánea, hacia otros, que ahora reconocemos como "dispositivos", y que permiten coordinar necesidades innatas al ser humano como las creadas por la sociedad actual.

En este apartado revisaremos algunos datos que muestran los indicadores de que la sociedad reclama una comunicación instantánea, actual y disponible.

Estudios relevantes han revelado que España tiene la mayor penetración de *smartphones* en el mercado europeo en lo que a telefonía móvil se refiere. En torno a un 70% de los usuarios móviles, posee un dispositivo inteligente. [5]

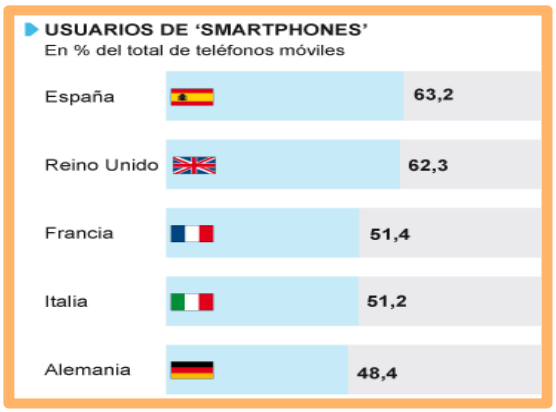


Figura 7: Ranking Países uso de *smartphones*

Además hemos podido comprobar cómo la teoría de "*always on*" es visible no solo en redes de telefonía fija, sino que incluso el acceso móvil encabeza el listado sin ninguna pretensión de descender en los próximos años. En la siguiente figura se muestran algunos valores que lo confirman. [6]

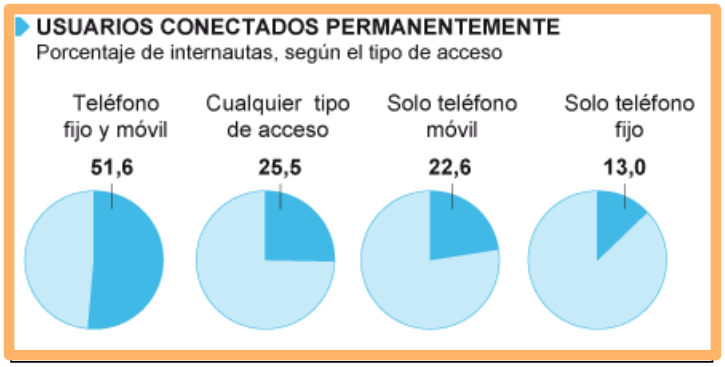


Figura 8: Porcentaje usuarios *always on* según el acceso

Como resultado de esta última afirmación, el acceso a la red móvil se incrementa diariamente en cuanto a direcciones IPv4 se refiere. Mientras que las peticiones de acceso a la red crecen casi de forma exponencial, la cantidad de accesos que permiten ofrecer servicios demandados, disminuye con la misma velocidad. De esta forma, surge la necesidad de aplicar la solución NAT que por el momento mantiene la paridad en los aspectos descritos. [7]

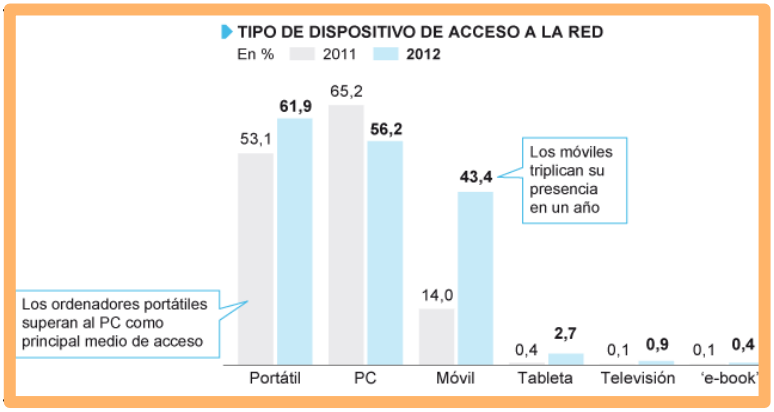


Figura 9: Distribución tipo de dispositivos de acceso a la red

El desarrollo de dispositivos que permitan el acceso a la red a través de protocolos superiores, como sería IPv6, se mantiene en constante evolución. Sin embargo, actualmente este acceso no está expandido debido a distintas razones, ya sean de interés comercial por parte de los proveedores de servicios o de los fabricantes, o como por problemas de arquitectura lógica.

2.3 Protocolos enrutamiento

En este apartado explicaremos el significado de los protocolos de enrutamiento que se emplean para poder asignar el direccionamiento adecuado en el acceso a Internet. Para ello es necesario subrayar brevemente cómo pueden los usuarios acceder al servicio determinado, recorriendo de forma transparente una serie de niveles hasta llegar al deseado. Los escalones a los que se hacen mención son los relativos a la conocida Torre OSI. [8]

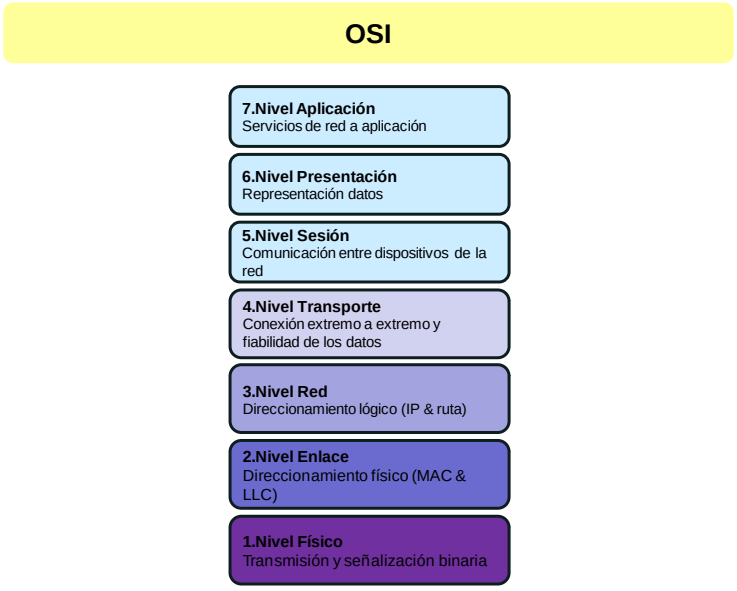


Figura 10: Modelo de Referencia OSI

Podríamos explicar detalladamente cada uno de los niveles que aparecen en la figura anterior, sin embargo es el nivel 3 dónde se asignan esas direcciones que permiten acceder al último nivel dónde por ejemplo el usuario puede acceder a servicios de HTTP, IP, POP3…

Para poder asignar esas direcciones se han creado una serie de organismos, como **RiRs**, encargados de gestionar, distribuir y registrar los recursos de numeración de Internet, ya sean de IPv4, IPv6 o Números de Sistemas Autónomos, dentro de las regiones asignadas. Básicamente existen **5 RIRs** distribuidas por cada uno de los continentes que se encargan de la administración de recursos globales de internet.

Según las últimas estadísticas mostradas por la RIPE NCC (región que se encarga de la zona europea), el número de direcciones IPv4 disponibles es de aproximadamente **16 millones**. A pesar de que la asignación de direcciones que se realiza a través de **IANA** (organización que distribuye el conjunto de direcciones IP a cada RIR) ha concluido, los distintos RIRs podrán usar ciertas direcciones siempre y cuando cumplan ciertos requisitos según los acuerdos establecidos. [9]

Una vez comprobada esa escasez de direcciones y hasta que la implantación del nuevo protocolo IPv6 sea una realidad, es necesario implementar temporalmente un mecanismo que provea el servicio. En este caso hablaremos de la técnica NAT, que junto con el los protocolos de enrutamiento utilizados en el dominio de la red, son responsables de encontrar las rutas para las entidades que requieren una dirección de red.

2.3.1 IPv4

Este protocolo tiene una capacidad limitada para permitir la expansión de Internet y por tanto no permite conectar miles de millones de dispositivos cuando sea apropiado. Proporciona un espacio de direcciones de 32 bits, que teóricamente son 4000 millones de direcciones globales únicas. No obstante, el número de direcciones globales de IPV4 que pueden utilizarse es bastante inferior debido a las ineficiencias en el uso y asignación de las mismas.

Esa limitación genera la necesidad de aplicar unos mecanismos, en este caso trataremos una de las variantes de NAT, que permite a través de la traducción de direcciones de red (IPv4 privadas), la prolongación de la vida útil de este protocolo.

Si nos fijamos en la cantidad de personas que ahora mismo posee más de un dispositivo que requiere una conexión a Internet, nos damos cuenta de que los 4 billones de direcciones públicas que otorga el protocolo IPv4 no son suficientes para ofrecer ese acceso a la red. [10]

2.3.2 IPv6

El protocolo IPv6 es una actualización del protocolo de Internet cuya principal motivación para el diseño y desarrollo fue la necesidad de ampliar el número de direcciones disponibles en Internet, permitiendo así la intercomunicación de miles de millones de nuevos usuarios. El uso de banda ancha para todos y tecnologías *always on*, determina la demanda del nuevo protocolo. Proporciona un espacio de direcciones de 128 bits, es decir, en torno a 340 sextillones de direcciones posibles. [10]

A largo plazo, IPV6 puede hacer que cada dispositivo IP sea más asequible, más poderoso e incluso consuma menos energía. Por ejemplo, permitirá una mayor duración de las baterías en dispositivos portátiles, otorgará a celdas telefónicas y dispositivos móviles, sus propias y permanentes direcciones. Además ofrecerá una mayor seguridad extremo a extremo.

Además este nuevo protocolo puede facilitar el cumplimiento de nuevos retos surgidos tras el despliegue de nuevos modelos extremo a extremo que requieren un acceso seguro y constante a las redes móviles. Es entonces, cuando el empleo del mecanismo de NAT podría inhibir el crecimiento de Internet, a través de esa traducción de direcciones.

Sin embargo, la mayor parte de los protocolos de transporte y/o aplicación necesitan pocos o ningún cambio para poder operar sobre este nuevo protocolo. Tanto el protocolo IPv4 como IPv6 presentan un encabezado de paquetes distinto, por lo que son interoperables entre sí. No obstante, la nueva actualización del protocolo permite minimizar el procesamiento de estos datos.

Es cierto que la solución más sencilla y optimizada sería implementar el direccionamiento IPv6 pero para ello debemos esperar que se convierta en la solución más estable y/o escalable. Algo que por el momento no podemos confirmar. Por lo tanto el empleo de NAT retrasará el agotamiento de direcciones de IPv4 públicas hasta que IPv6 se adopta adecuadamente.

Muchas son las encuestas que se han realizado acerca de la penetración actual y futura de este nuevo protocolo. Cabe destacar aquella realizada por TNO y GNKS en colaboración con varias entidades como RIPE, en las que se demuestra que gran parte de proveedores de internet tienen claro que van a promocionar IPv6 a los usuarios, ya sea por satisfacer necesidades futuras o por el evidente agotamiento de direcciones de internet de la versión anterior. Además mientras que algunos no pueden afrontar el gasto de la nueva asignación IPv6, otros que ya la tienen planteada, cuentan con un escaso soporte de los fabricantes. En líneas generales, la lenta implementación de este protocolo en entornos de producción se debe a la escasa demanda de los usuarios.

2.3.3 NAT

Puesto que ambos protocolos de internet están destinados a convivir durante bastantes años mientras se completa la implantación del nuevo protocolo IPv6, existen unos mecanismos que permitirán esa migración progresiva.

Existe un gran número de técnicas que ayudan a solucionar este problema, y la mayor parte están basadas en la traducción de direcciones de internet. Más conocido como NAT (Network Address Translation), este mecanismo asigna una dirección IP única en múltiples direcciones IP privadas que pueden utilizarse internamente en una red privada.

Solemos aplicar esta solución cuando uno de los nodos soporta únicamente la versión IPv4 del protocolo e intenta comunicarse con otro nodo que sólo soporta IPv6.

En las próximas líneas explicaremos algunas versiones mejoradas de este mecanismo, recordando que el papel fundamental del mecanismo de NAT consiste en alterar las direcciones de la cabecera IP de un paquete.

En este proyecto, el objeto consiste en aplicar esta técnica en la red de una operadora móvil, comunicando de forma global la red LAN con la red WAN (Internet en este caso). Una idea sencilla del funcionamiento se presenta en la siguiente figura:

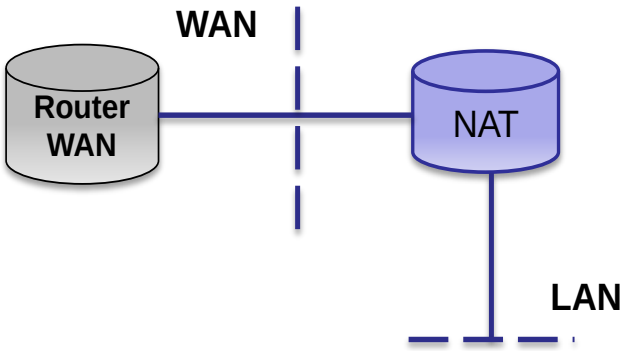


Figura 11: Arquitectura NAT

Las direcciones de la red de una operadora móvil cualquiera, evidentemente son direcciones privadas que pertenecen a distintas clases [11] .Puesto que no es posible conectar distintas redes privadas a través de Internet, dos usuarios de distintas redes privadas podrían emplear el mismo direccionamiento privado sin riesgo de que se generara un conflicto.

Sin embargo, cuando un usuario de una red privada necesita comunicarse con otro de otra red privada, es necesario que cada uno pueda conectarse a través de una dirección pública provista en esa red privada, y que sea alcanzable para poder establecer esa comunicación. Será el *router* por su propia definición, quién tendrá acceso a esa *Gateway* (que en nuestro caso es el equipo encargado de realizar NAT) que le encamine hacia el extremo que desea comunicarse.

Sabemos que NAT es un método por el que las direcciones IP se asignan de un campo a otro en un intento de proporcionar encaminamiento transparente a los equipos *hosts* [12].

La necesidad de aplicar una traducción de direcciones IP surge cuando las direcciones IP internas de una red no se pueden utilizar fuera de la red, ya sea porque no son válidas para el uso exterior, o debido a que el direccionamiento interno debe mantenerse oculto desde la red externa

Los dispositivos que aplican NAT tratan de proporcionar una solución de enrutamiento transparente a las máquinas finales, comunicándose desde dominios de direcciones dispares. A través de la modificación de las direcciones de nodos finales en ruta y manteniendo el estado de estas actualizaciones, logramos que las peticiones se dirijan al nodo final correcto sea cual sea el ámbito en el que se encuentre, sea en este caso IPv6.

Para identificar extremos de una comunicación, es recomendable emplear soluciones aplicadas a DNS, ya que así evitamos traducir el contenido de *payload* pues no se cambia de dirección IP, de lo que se demuestra que no siempre es bueno emplear NAT según lo que necesitemos comprobar.

Es necesario comentar que el enrutamiento que aplica el mecanismo NAT es de tipo transparente. Combina direcciones (en este caso de dominio IPv4 e IPv6) a través de modificaciones del contenido de la cabecera IP, para que sea válida hacia el nuevo dominio. Es decir que emplea un enrutamiento distinto del que aplicaría un enrutador tradicional (*router)*, que sólo encamina direcciones de un propio dominio, por ejemplo, direcciones de tipo IPv4. A continuación mostramos el tipo de enrutamiento que aplica el mecanismo NAT.

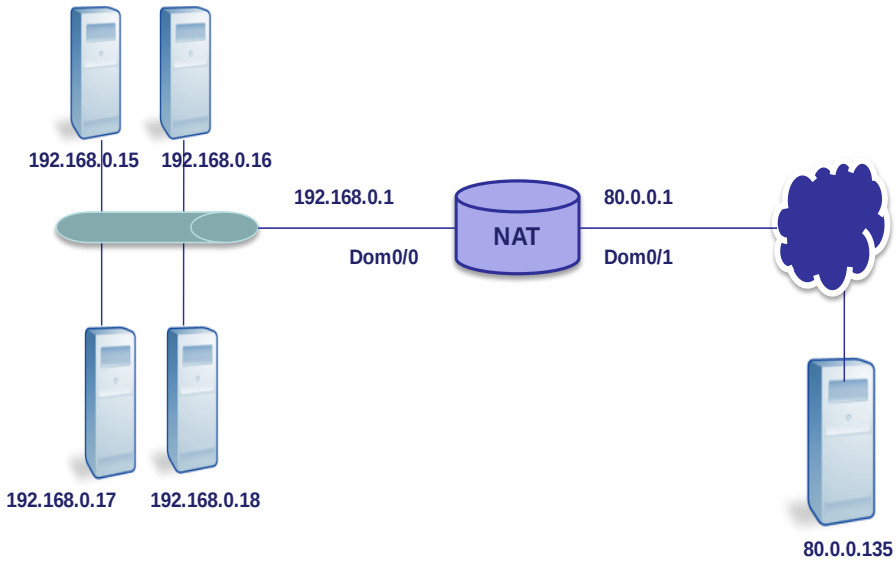


Figura 12: Funcionamiento arquitectura NAT

Desde interfaces internas y externas de los *routers* CPE, de direcciones IPv4 privadas, se debe tener cuidado de que estas direcciones IP no se superpongan, de lo contrario, podría causar problemas de enrutamiento. En este caso, el proveedor de servicios utilizará 10.0.0.0 / 8 de bloque para asignar direcciones a los clientes. El tráfico interesante para NAT será el tráfico con dirección de origen de la red 192.168.0.1/24 pues la CPE utiliza esta máscara para hacer frente a los dispositivos de la red.

Algunas de las técnicas empleadas para poder llevar a cabo la migración del nuevo protocolo IPv6, son las siguientes:

- NAT44
- CGNAT444
- NAT46
- NAT64 + DNS 64
- DUAL STACK
- DS LITE (Dual Stack Lite)

2.3.4 NAT44

Es un mecanismo que se ha adoptado ampliamente para hacer frente al agotamiento de direcciones IPv4 [13]. Se traduce una dirección IPv4 pública en muchas direcciones IPv4 privadas. Se aplica en dispositivos con conexión a internet que sólo soportan IPv4. Es decir, estos dispositivos acceden a un servicio de tipo IPv4 a través de una red de tipo IPv4.

La integración de NAT44 puede aplicarse de varias formas:

Forma independiente: sobre todo para el caso de tener problemas con direcciones IP estáticas, empleadas en el HLR/HSS, AAA o DHCP.

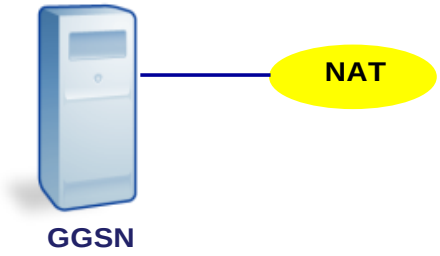


Figura 13: Integración NAT44 independiente

Forma integrada: para el caso en el que las direcciones IP son conocidas por el Gateway, GGSN, y que pueden usarse para hacer el disparo de NAT

Figura 14: Integración NAT44 independiente

La solución de NAT no es tan trivial o simple como parece a simple vista. Existen unos factores previos que deben considerarse antes de comenzar su desarrollo. Ciertas aplicaciones que utilizan las direcciones IP en el "payload", es decir, en la carga útil de la aplicación (FTP, SIP, RTSP), deben tener una traducción más elaborada. Y otras aplicaciones contienen especificaciones adicionales para habilitar los modos de operación NAT44, como podría ser aplicaciones P2P basadas en juegos online.

En esta técnica encontramos también definido lo que se conoce como PAT (Port Address Translation) que consiste en la traducción de ambas direcciones públicas (tanto la pública como la privada) así como los números de puertos. La traducción se lleva a cabo en un dispositivo, normalmente un firewall o un router, que utiliza tablas de traducción con estado para asignar las direcciones IP privadas (ocultas) en una única dirección IP. Así redirige los paquetes IP salientes en la salida, de modo que parecen originarse desde el dispositivo.

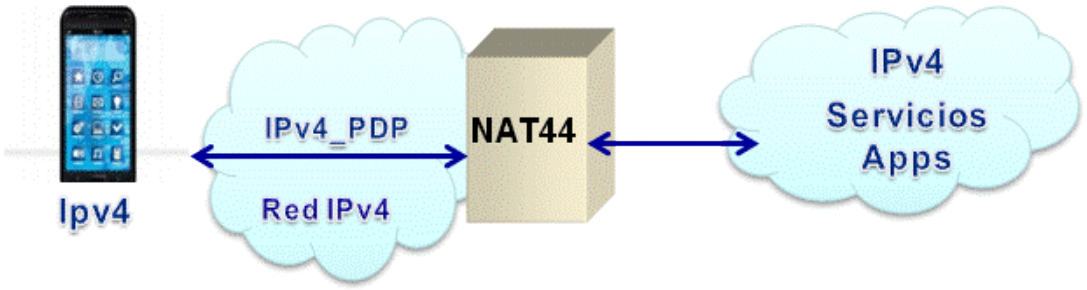


Figura 15: Arquitectura solución NAT44

A medida que el modelo de dispositivos cambia, el aumento del uso de internet y la conectividad de la nube va siendo más real y las direcciones IPv4 alcanzan un valor máximo que no puede ampliarse.

Algunas de las aplicaciones/servicios no pueden ofrecerse a través de una implementación básica de NAT, requieren unas soluciones basadas en mecanismos que alteren puertos y/o direcciones IP.

Las técnicas que van a ayudar a asignar las direcciones a la plataforma de NAT son múltiples y variadas aunque las que hemos elegido en este proyecto se basan en dos:

- Una técnica que se conoce como **asignación de puertos**, en la que los puertos y las direcciones IP se han asignado de forma estática, permitiendo que se establezcan las comunicaciones de los servidores externos con los servicios que se prestan en una operadora móvil. Se envían los paquetes IP que atraviesan la plataforma de NAT a un puerto determinado de un host que se encuentra detrás de la plataforma. Para poder enviar esos paquetes nos basamos en el número de puerto por el que recibió NAT. Esto permite a los servidores operar en lo que se conoce como *well known ports* (<1024), asignados permanentemente a un puerto exterior.

- Por otro lado se han aplicado **mecanismos a nivel de aplicación** conocidos como ALGs para poder conseguir aplicar NAT a ciertas aplicaciones.

2.3.5 CGN (NAT444)

Esta propuesta de diseño también permite retrasar la transición entre el protocolo IPv4 y el nivel superior IPv6. Durante el periodo de coexistencia de ambos protocolos, este diseño permite simplificar la gestión de servicios del usuario final. El proceso es sencillo, se traducen direcciones del dominio de la red privada en direcciones IPv4, permitiendo intercambiar conjuntos de direcciones públicas, entre varios puntos finales.

Se podría definir como NAT444, ya que las conexiones de algunos clientes a los servidores públicos atravesarían tres dominios basados en IPv4 [14]. Es decir, primeramente se establecería la conexión en la red privada del cliente, a continuación accederíamos a la red privada de la compañía y finalmente accederíamos a la red pública.

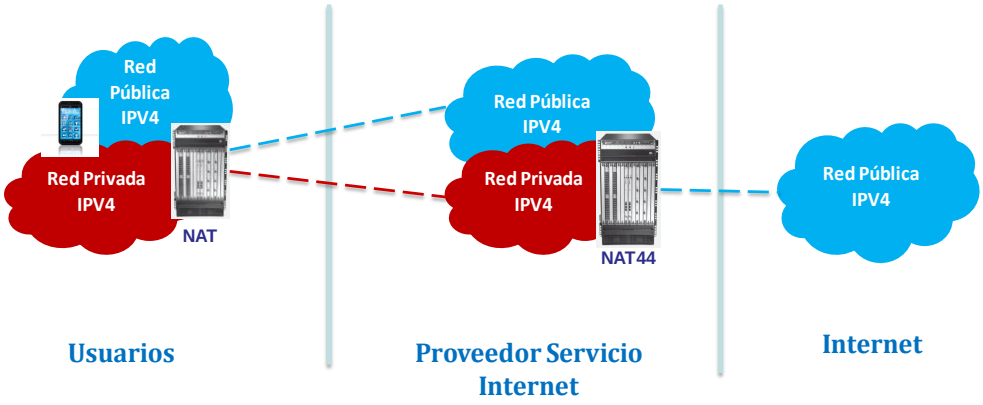


Figura 16: Arquitectura solución NAT444

2.3.6 NAT46

Esta técnica permite la comunicación de un cliente sólo-IPv4 y un servidor sólo-IPv6 a través de la traducción de cabeceras de ambos protocolos, tanto en un sentido como en otro. Básicamente se traduce una dirección IPv4 en otra IPv6, para proporcionar a los dispositivos basados en IPv4 conectividad a las aplicaciones IPv6 sobre una red IPv4.

Este tipo de solución de las AFT (Address Family Translation) alarga la vida de las direcciones IPv4. [15] Lo que se conoce como NAT46 Gateway se desarrolla en el *core* de la red de paquetes, y suele estar integrado en el GGSN dado que una de sus funciones principales consiste en la conversión de protocolos UMTS a otros de otras redes. Para poder implementar esta solución es necesario además emplear NAT44 de forma conjunta.

Para este proyecto se considera una opción con demasiados inconvenientes para solucionar temporalmente el problema del agotamiento de direcciones IPv4.

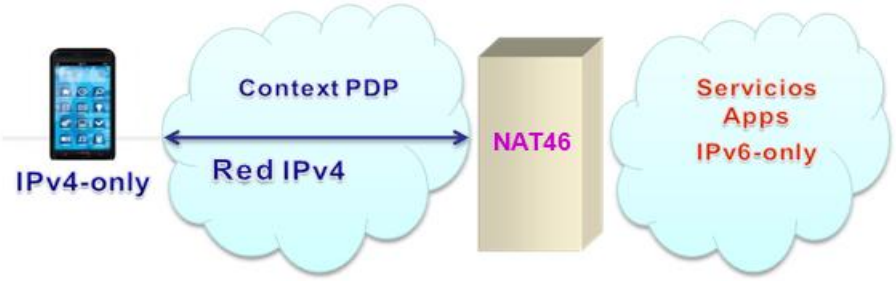


Figura 17: Arquitectura solución NAT46

2.3.7 NAT64+DNS64

En este tipo de solución se permite la comunicación de un cliente sólo-IPv6 y un servidor sólo-IPv4 a través de la traducción de cabeceras de ambos protocolos, tanto en un sentido como en otro. Para una red de gran envergadura es necesario un DNS-64 para que pueda asignar o resolver el dominio de los nombres asignados a cada dirección. Este mecanismo consta de dos partes, un equipo DNS_64 encargado de resolver las peticiones de los dispositivos IPv4-only, además de una pasarela (NAT64_*gateway*) encargada de corresponder las direcciones IPv6 con las direcciones del mundo IPv4 [16]. Este último equipo se encuentra integrado normalmente en el GGSN al inicio de la Red Core de Paquetes de la red móvil.

A pesar de ser una buena solución para radicar el problema que consigue ahorrar en asignación de direcciones IPv4 de los dispositivos, es demasiado drástica para comenzar con el traspaso de direcciones IP. Esta opción implicaría una actualización tanto de dispositivos como de nodos de red para soportar el nuevo direccionamiento IPv6. Por último y no menos importante, es importante destacar que requiere técnicas conjuntas basadas en NAT transversal como son ALG64 o Proxy64, donde el desarrollo comercial no se ha visto extendido. Y por lo tanto, muchas aplicaciones, como podrían ser *Skype* o *Spotify* basados en IPSec, no soportarían este tipo de mecanismo.

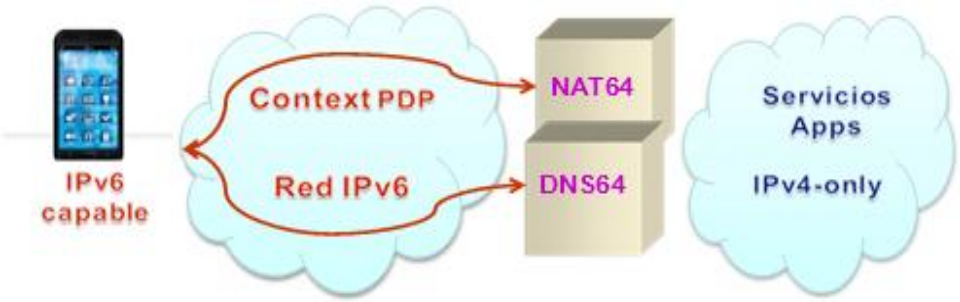


Figura 18: Arquitectura solución NAT46+DNS64

2.3.8 DUAL STACK

Esta solución implementa lo que se conoce como la doble pila, es decir, se integran en cada nodo de la red, las pilas de ambos protocolos, IPv4 e IPv6. Cada nodo con doble pila tendrá dos direcciones de red, una IPv4 y otra IPv6. Así esos nodos tienen la capacidad de enviar y recibir tanto paquetes IPv4 como IPv6.

Sin embargo no tienen porqué estar activadas ambas pilas de forma simultánea. Es decir, pueden habilitarse ambas pilas, o activar pilaIPv4 y desactivar pilaIPv6, o viceversa. Especialmente, si desactivamos la implementación del protocolo IPv6 en la pila IPv6/IPv4, funcionará únicamente con nodos IPv4, y por el contrario, si deshabilitamos en la pila la funcionalidad para el protocolo IPv4, sólo podrán comunicarse nodos IPv6.

Positivamente es una solución fácilmente desplegable además de estar extensamente soportada. Sin embargo, no es muy eficiente en cuanto a optimización de red, pues la topología de red requiere que ambas tablas de encaminamiento, tanto la relativa a IPv4 como para IPv6, necesiten actualizarse. Esta es una característica que podría suponer problemas en las configuraciones de red, además de la necesidad de integrar ambas versiones de protocolos de internet.

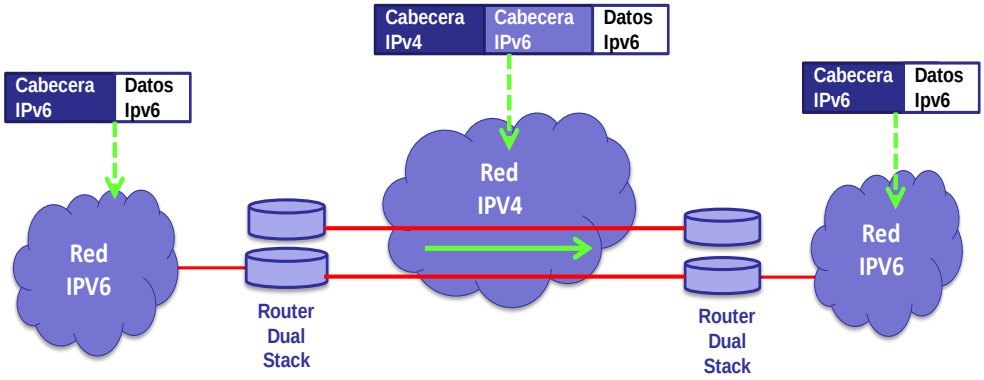


Figura 19: Arquitectura solución Dual Stack

2.3.9 DS LITE (Dual Stack Lite)

Permite al proveedor de servicios compartir las direcciones públicas (IPv4) entre los distintos clientes a través de la combinación de técnicas de tunelización y el mecanismo de NAT. Permite que múltiples dispositivos de acceso compartan la misma dirección IPv4 privada. En lugar de iniciar el túnel en el dispositivo de acceso, se extienden lógicamente los túneles de acceso más allá del PDN hacia el AFTR elegido, empleando un mecanismo de efecto túnel con una semántica para llevar el estado del contexto relacionado con el tráfico encapsulado [17].

Extiende túneles de acceso existentes más allá de la pasarela de acceso (que podría ser cualquier PDN-GW) a un NAT tipo IPv4, empleando IPv4Softwires con identificadores de contexto embebidos que identifican de forma exclusiva el sistema externo al que pertenecen los paquetes del túnel. Por ello la pasarela de acceso, PDN, identifica qué parte del tráfico requiere NAT a través de unas políticas locales y enviará/recibirá ese flujo hacia/desde ese software.

DS-Lite: Aprovecha los túneles IPv4 en IPv6 (u otros túneles) para transportar el tráfico de IPv4 de la red del cliente al router de la familia AFTR. De esta forma, un softwire entre el AFTR elegido (NAT44 en este caso) y el dispositivo de acceso se utiliza para los propósitos de reenvío y enrutamiento de tráfico, así permite compartir direcciones privadas IPv4 entre los distintos clientes dentro de la red de servicios.

Softwire Protocol: Es un tipo de protocolo de tunelización que crea un cable virtual encapsulando otro protocolo como si fuera un enlace anónimo de punto-a-punto de bajo nivel.

Este mecanismo consiste en un túnel punto a punto entre el dispositivo y el GGSN, además de añadir un túnel *Softwire,* como podría ser un túnel GRE, entre el GGSN y el equipo que se encargue de aplicar el mecanismo CGN (Carrier Grade NAT). Una vez establecido el túnel, el equipo GGSN asocia los contextos PDPs con túneles GREs empleando un identificador único, que dependerán de las necesidades del operador, podrían ser por ejemplo las claves GRE. El equipo que aplica el mecanismo CGN termina el túnel, y en caso de que sea necesario aplicaría otro tipo de NAT44.

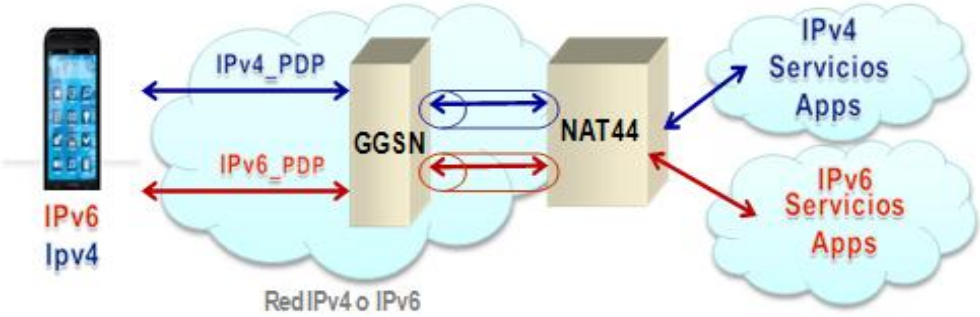


Figura 20: Arquitectura solución Dual Stack Lite

Este enfoque se apoya en la superposición de direcciones IPv4 en la red de acceso, y no requiere cambios según sea el dispositivo o la arquitectura de acceso. Esta opción no añade información adicional en la cabecera en la red de acceso debido a la tunelización. Además como la dirección IPv4 asignada para el dispositivo no se utiliza para el reenvío de paquetes, permite una superposición de direcciones.

La limitación que tiene este mecanismo de NAT impide en muchas ocasiones soportar por sí solo las aplicaciones de forma transparente y debe coexistir con pasarelas a nivel de aplicación (ALGs). En esta técnica es recomendable emplear soluciones aplicadas a DNS para identificar extremos de una comunicación. Así evitamos traducir el contenido de *payload* pues no se cambia de dirección IP.

2.4 Application Layer Gateway

La mayor parte de servicios de navegación suelen funcionar con servicios de NAT básicos. Sin embargo, existen servicios específicos en los que los servicios son más complejos y es necesario implementar plataformas más sofisticadas. Principalmente son aquellos que incluyen direcciones IP con puertos TCP/UDP en el *payload* De este modo, surge la necesidad de integrar los recursos ALGs específicos para esos tipos de tráfico.

Definimos ALG como las pasarelas a nivel de aplicación que actúan como agentes de traducción para aplicaciones específicas. Permiten que una aplicación en un servidor de un dominio de direcciones pueda conectarse a su contraparte para que el host se ejecute en un ámbito distinto.

Por lo tanto cualquier aplicación que haga uso de direcciones IP en capas más altas que la relativa a la de nivel del protocolo de internet, no funcionará adecuadamente sin aplicar estos mecanismos.

Estas aplicaciones requieren direcciones y puertos IP para poder atravesar el equipo de NAT. Estos ALGs revisan los paquetes IP y cambian los puertos/direcciones dentro del payload. Se asigna esta solución para determinadas aplicaciones que no soportan NAT de forma transparente. Es decir que con el cambio que se aplica en estas cabeceras, esas aplicaciones pueden acceder al equipo de NAT.

En este apartado describiremos brevemente cada una de las aplicaciones que se han probado junto con el mecanismo de NAT en el desarrollo de este proyecto.

2.4.1 HTTP

Es el protocolo orientado a transacciones siguiendo el esquema petición-respuesta entre un cliente y un servidor [18]. El que realiza la petición se le conoce como “user agent". La información transmitida se conoce como recurso y se identifica a través del localizador uniforme de recursos (URL). Los recursos pueden ser archivos, resultado de un programa, consulta de base de datos…

Definido como un protocolo de transferencia de hipertexto, se basa en un protocolo de nivel de aplicación para sistemas de información distribuidos. Es genérico y estático y puede emplearse como sistema de gestión de objetos distribuidos, a través de la extensión de sus métodos de petición, códigos de error y encabezados. La característica más importante es la escritura y la negociación de la representación de datos, permitiendo así una independencia de los datos que se transfieren. El uso de campos de encabezados enviados en las transacciones HTTP le otorga una gran flexibilidad al protocolo. En estos campos se envía información descriptiva de la transacción.

2.4.2 TCP

Este protocolo de control de transmisión se utiliza como un protocolo host-host, siendo muy fiable entre miembros de redes de comunicación de ordenadores intercambiando paquetes. Es un protocolo orientado a conexión, fiable entre dos extremos [19]. Diseñado para encajar en una jerarquía de capas que soportan aplicaciones sobre múltiples redes. Proporciona mecanismos para obtener una comunicación fiable entre los pares de procesos en computadoras, aunque no existen demasiadas comprobaciones en cuanto a la fiabilidad de los protocolos de comunicación por debajo de la capa TCP.

Es un protocolo que debería ser capaz de operar en todo tipo de sistemas de comunicación. El propósito principal de este protocolo consiste en proporcionar un servicio de conexión fiable.

Como veremos en el desarrollo del proyecto las sesiones TCP/UDP se identifican de forma única por la pareja (IPorigen, puertoOrigen TCP/UDP) junto con (IPdestino, puertoDestino TCP/UDP).

2.4.3 IMAP

Es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet [20]. Este es el protocolo de acceso a mensajes de Internet que permite a un cliente acceder y manipular los mensajes de correo electrónico en un servidor. Además ofrece la opción de manipular los buzones de manera funcionalmente equivalente a carpetas locales.

Incluye las operaciones para creación, eliminación, cambio de nombre de buzones de correo, comprobar si hay nuevos mensajes, análisis, búsqueda, obtención de los atributos de los mensajes, textos y partes de los mismos e incluso permite la sincronización de un cliente desconectado con el servidor. No obstante, sólo soporta un único servidor sin especificar cuál es el medio de publicación de correo electrónico aunque un gran número de transacciones.

Es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet. A través de este protocolo se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una de las ventajas que tiene con respecto a otros protocolos empleados para obtener correos desde un servidor, es el hecho de poder definir carpetas del lado del servidor, permitiendo visualizar mensajes de manera remota sin descargar los mensajes.

2.4.4 POP3

El protocolo de Oficina de Correo es un protocolo de red que se utiliza en clientes locales de correo electrónico para obtener mensajes de correo electrónico almacenados en un servidor remoto [21].

Basándonos en el modelo basado en la torre OSI, resulta ser un protocolo de nivel de aplicación que se basa en la comunicación del protocolo TCP en el puerto 110.

Cuando el protocolo necesita entrar al buzón, se conecta mediante el servidor de POP3, recupera la información que necesita para después cerrar la conexión. De esta forma, si posteriormente es necesario volver a entrar al buzón de entrada, se creará una nueva conexión… A través de conexiones de baja velocidad permite a los clientes descargar su correo electrónico siempre que haya conexión por eso es útil para recibir el correo pero no para enviarlo. De esta forma una vez descargado puede revisarse ese correo estando desconectado del servidor que ofrece el correo electrónico.

2.4.5 SSL

El objetivo principal del protocolo SSL es proporcionar privacidad y fiabilidad entre dos aplicaciones que se comunican [22]. Se establece en las capas en la parte superior de algunos protocolos de transporte como por ejemplo TCP, y otros de aplicación como HTTP, SMTP, NNTP… En estos últimos se aplica para asegurar las páginas de tipo World Wide Web en todas sus diversas formas.

Además se emplea como método estándar para proteger la señalización de aplicaciones con SIP, como para proveer autenticación y cifrado de la señalización asociada con VoIP o incluso para tunelizar una red completa y crear una red privada virtual.

El funcionamiento radica en el intercambio de registros que pueden ser comprimidos, cifrados y empaquetaos con códigos de autenticación. Cada registro conserva un campo que especifica el protocolo del nivel superior que están usando. Para iniciar la conexión tanto cliente y servidor intercambian mensajes en los que se identifican los parámetros necesarios, según las claves públicas designadas.

Especialmente tanto cliente y servidor negocian una clave a partir de varios mecanismos cuidadosamente aleatorios.

2.4.6 IPSEC

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet, cifrando cada paquete IP en un flujo de datos [23].

Aporta seguridad a las redes IP ya que es capaz de bloquear ataques contra redes no protegidas, o también protegiendo extremos que demandan una comunicación a través del establecimiento de túneles seguros. Además es un protocolo interoperable que no afecta a los elementos que lo implementan y es adaptable a nuevos algoritmos de cifrado.

Su característica principal se basa en el uso de una cabecera de autenticación AH, en la que se integran y autentican los datagramas IP, así como el uso de otra cabecera de seguridad ESP, que aporta el cifrado de las comunicaciones. Ambas cabeceras se usan para proteger esas comunicaciones IP.

Todas estas técnicas destinadas a mantener las direcciones de punto final de un paquete IP no son operables con el mecanismo de NAT simplemente, si no que es necesario desarrollar otra ALG que permita esa interoperabilidad.

2.4.7 P2P: BitTorrent

Tal y como comprobaremos en el desarrollo de las pruebas realizadas, el protocolo BitTorrent está basado en una red de nodos que conservan el mismo comportamiento entre unos y otros. Es decir, el usuario que realizará la petición y los nodos a los que llega esa petición, actuarán tanto uno como cliente y servidor. Intercambiarán entre ellos un gran número de archivos algo que proporciona redundancia ante determinados problemas de la red, aunque dificulta el seguimiento del origen del archivo que circula por el entramado de nodos.

La idea es no almacenar un archivo en un servidor fijo, si no que por el contrario, estará compartiéndose entre los usuarios que forman la red compartida. Es decir, es como si se dispusiera de varios servidores algo muy práctico para emplearlo en dispositivos con poco ancho de banda, como pueden ser los *smartphones,* quienes pueden distribuir archivos (un ejemplo claro seria el *streaming)* hacia muchos receptores.

El funcionamiento de este protocolo se iniciaría con la creación de un archivo tipo, (en nuestro caso será *utorrent,* es el servidor original que dispone el archivo a compartir) por parte del usuario que quiere compartir determinado archivo. Después debería incluirlo en la red empleando un nodo que forme parte de la red BitTorrent.

Así si un usuario desea descargar el archivo, obtendrían el archivo tipo creado, para llegar a ser el nuevo cliente que porta el archivo y que debe crear otro nodo tipo para compartir los archivos con el usuario inicial y con otros nuevos usuarios que requieran los archivos, algo que también sucedería con el usuario original.

3 DESARROLLO DEL PROYECTO

El objetivo de este proyecto consiste analizar el comportamiento al aplicar la técnica NAT44 en el acceso al servicio de Internet en una operadora móvil a través de la definición de unas pruebas en un entorno controlado. A través del desarrollo de este análisis se obtendrán unos resultados donde comprobaremos si la implementación de esta técnica de traducción es válida para los servicios demandados por los usuarios de esta red.

3.1 Evaluamos los equipos

En este apartado definiremos los criterios necesarios para poder elegir el equipo que se encargue de realizar óptimamente la traducción de direcciones de internet que posteriormente ofrecerá el servicio de Internet.

3.1.1 Criterios de Diseño

Los criterios en los que se ha basado la elección de la plataforma traductora son los que se muestran a continuación:

Volumen de tráfico

Para poder implementar esta solución nos hemos basado en criterios de tráfico. El criterio básico que debería soportar el equipo que forme parte de la implementación de esta solución debería tener la capacidad mínima de soportar el flujo de tráfico que mantiene un equipo GGSN.

Si establecemos un comportamiento conservador de la capacidad soportada con la que habría que dimensionar los equipos, esta capacidad debería ser el doble de lo esperado según las previsiones de tráfico de usuario calculadas por el proveedor del servicio, en este caso una operadora móvil.

Flexibilidad de adaptación

Continuando con el criterio anterior, podemos destacar que otro de los criterios importante, es la flexibilidad de añadir o disminuir capacidad en cuanto al volumen de usuarios. Por ejemplo, un equipo sería muy flexible si a pesar de haber añadido inicialmente una capacidad inicial, es capaz de añadir módulos a medida que el número de usuarios aumenta y se requiere por lo tanto una mayor capacidad de estos nodos.

Si bien esta es una cualidad, podría contener cierto riesgo si la conducimos al límite, confiando que justo en el momento que carezcamos de esa capacidad el equipo va a responder positivamente.

Sesiones Concurrentes

Este criterio está ligado con el anterior básicamente por la propia definición de los servicios que debe soportar el equipo elegido basado en NAT y que sustituye direcciones IP además del número de puerto origen del tráfico del usuario.

Este equipo deberá tener una capacidad de sesiones concurrentes que permita emplear un número limitado de direcciones IP públicas para un espacio de direcciones IP privadas mucho mayor.

Basándonos únicamente en terminales de usuario comprobamos que las aplicaciones de las que hacen uso albergan cada vez más sesiones concurrentes. Suponiendo que una operadora móvil tiene unos 300 mil abonados con servicios de datos contratados, el equipo debería soportar esas conexiones mínimamente.

Si además se tiene en cuenta que el número de conexiones es sensible a crecimiento, debido a conexiones de servicios auxiliares por motivos de sincronización, servicios multiusuario, como juegos online, o en el mejor de los casos ampliar la cuota de mercado de la operadora con nuevos clientes… sería necesario incrementar esa capacidad de forma escalada a medida que se producen los eventos.

Gestión de direcciones IP

La plataforma elegida para solucionar el problema de direccionamiento debería poseer la flexibilidad en cuanto a la aplicación de lógicas de traducción según el servicio. De esa forma el equipo tendría la capacidad de integración con otros sistemas terceros de gestión de direcciones IP. El tráfico entrante que se genere en el uso de Internet también debe ser gestionado por las plataformas de NAT ya que asignarán no solo las direcciones de su propia red, sino de las peticiones que accedan del exterior.

Continuidad del servicio

El ultimo criterio que debería aprobar el equipo de NAT, seria poder disponer del servicio de internet elegido independientemente de la arquitectura implementada.

Podríamos optar por implementar una arquitectura NAT patrón a la que pudiéramos incluir sistemas internos que aseguren la disponibilidad de servicios.

Por el contrario, existe otra opción en la que la arquitectura en donde la capacidad de asignación de servicio sea la mayor posible.

De esta forma se maximizan el número de casos en los que existe una indisponibilidad de la arquitectura, logrando la continuidad de servicio y facilitando la operación local de sistemas sin afectar al servicio.

3.1.2 Criterios técnicos

La solución aportada por esta plataforma debe cumplir ciertos requisitos técnicos que se describen a continuación:

- Solucionar el problema del agotamiento de las direcciones públicas tipo IPv4 adoptando ciertas recomendaciones que aparecen en las RFC4787.

- Deben aplicar las claves necesarias a aquellas aplicaciones que necesitan un tratamiento especial para poder funcionar con este mecanismo NAT44.

- Debe soportar IPv6 para complementar la migración que deba realizarse posteriormente.

- No es conveniente que añada cierta latencia al tráfico de usuario por llevar a cabo las traducciones de una dirección pública a una dirección privada.

- Debería ajustarse para provisionar la capacidad de tráfico requerido hasta que la migración hacia direccionamiento IPv6 sea inminente.

- Debe comprender un buen nivel de flexibilidad tal que pueda desarrollarse en caso de que el escenario de acceso a internet a través de la interfaz Gi se modifique con facilidad.

- Debe ser simple en operación y administración.

No obstante, el equipo elegido sería incapaz de controlar la totalidad de las asignaciones ip+puerto, por lo tanto sería necesario establecer una sincronización de las tablas de NAT para los casos de mayor volumen de tráfico, o en el caso de conexiones concurrentes, para evitar así la pérdida del servicio. Debería existir escalabilidad en cuanto a la capacidad del proceso de las políticas de seguridad.

3.1.3 Modelo elegido

En la elección de la plataforma que realizará la traducción de direcciones no sólo han influido los criterios en el apartado anterior, sino también ciertos criterios subjetivos. La mayor parte estos últimos están relacionados con los costes empresariales, acuerdos comerciales con determinados fabricantes, y parámetros que permanecen fuera del alcance de este proyecto.

Para el objeto de nuestro proyecto definiremos esta plataforma como **NATBOX** y comenzaremos a describir a continuación las cualidades de las que dispone.

3.1.3.1 Características técnicas

El chasis encargado de realizar el servicio de NAT que posee una redundancia máxima en cuanto a procesadoras y puertos se refiere, dispone de las siguientes tarjetas y puertos:

- Contiene 2 tarjetas procesadoras: encargadas de manipular el tráfico de usuario.

- Son 4 fuentes DC de 4100W, a través de las que se conectará el equipo a la red eléctrica.

- Posee 2 ventiladores y filtro necesarios para el funcionamiento de una plataforma eléctrica.

- Es un software necesario quién controla de forma inteligente la plataforma.

- El cerebro de la plataforma son 2 tarjetas MIC (a media altura) con 4 puertos 10G y los denominados SPF (single point of failure), necesarios para comprobar si ha existido pérdida de servicio a través de alarmas que envía el equipo.

- Existen además 2 tarjetas MIC (a media altura) con 20 puertos de 1G y 10 puertos de fibra y otros 10 de cobre por tarjeta, que almacenan otro tipo de tráfico que no es el propio de internet.

- Final y principalmente, el equipo cuenta con 2 módulos de servicios DPC implementados con unas licencias que soportan las transacciones de NAT más importantes.

A continuación mostramos el chasis del equipo y nos permite comprobar más detalladamente dónde se encuentran los elementos que realizan el balanceo [24].

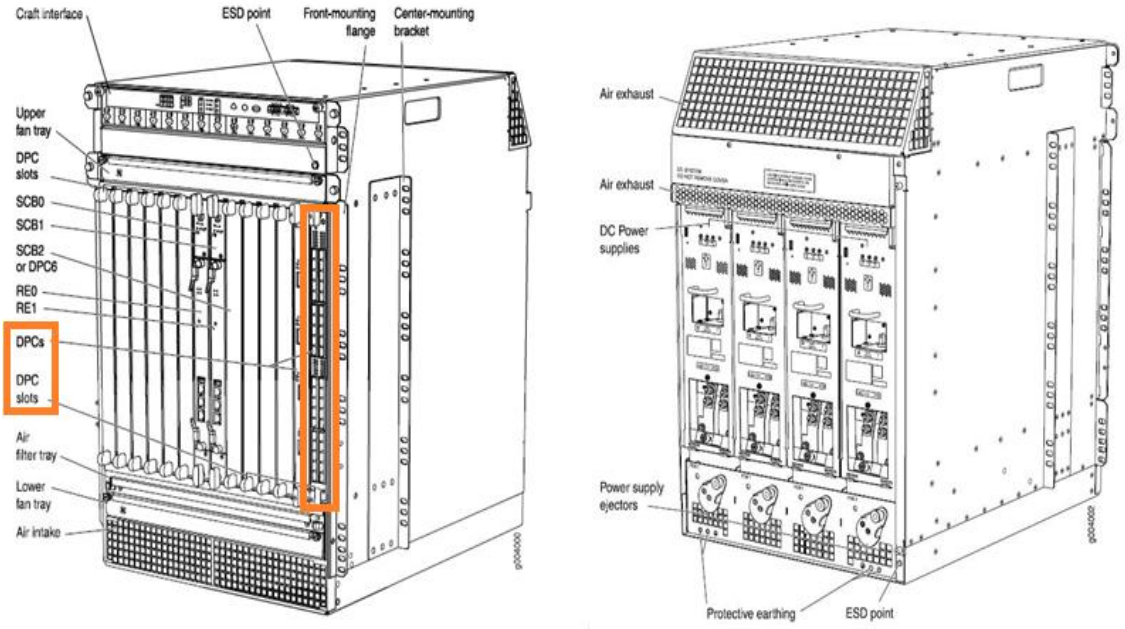


Figura 21: Chasis delantero y trasero equipo NATBOX

3.1.3.2 Características funcionales

Las características principales del equipo NATBOX se basan principalmente en:

- Contiene la funcionalidad de *router* de alta densidad de puertos que realiza funcionalidades a nivel 2 y 3.

- Cuenta con 12 slots que procesan el tráfico y otros 2 slots que se conocen como slots de control para evitar perder el control en caso de caída de una de las tarjetas. Cada uno de los slots está definido para soportar un tráfico de 120 Gbps.

- Puede desarrollar un diseño redundante. Explicaremos más adelante que pueden colocarse pares de equipos para controlar la congestión de tráfico a través de una arquitectura basada en la redundancia geográfica.

- La velocidad de las tarjetas RAM cuenta con velocidades que permiten soportar el servicio de NAT hasta los 3Tbps.

❖ Esta plataforma cuenta con multitud de tarjetas que le permiten operar el servicio:

- Tarjetas MPC2-3D con puertos de 10Gbps y 1Gbps.
- Tarjetas MIC-3D cada una de 4 puertos de 10G para utilizar dos interfaces 10G de entrada y otros dos interfaces de 10G de salida.

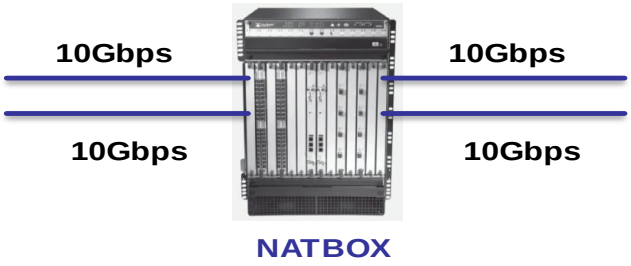


Figura 22: Distribución velocidad puertos y canales del equipo NATBOX

- Tarjetas MIC-3D de 20 puertos de 1GE para realizar conexiones adicionales que requiera el equipo. Estos puertos se emplean para conectarse a través de la gestión de fuera de banda, es decir, para poder acceder al equipo con equipos que no forman parte de la arquitectura que habilita el servicio.

- Por último y no menos importante, cuenta con los módulos MS-DPC encargados de realizar las labores de NAT. Deben soportar unas transacciones iniciales tales que permitan suministrar el tráfico de las sesiones de usuarios que realicen NAT. Para trabajos futuros en los que la red de la operadora se vea expandida, y gracias a la escalabilidad de esta máquina podemos ampliar esas transacciones.

El software que utiliza el equipo NAT se basa en un **kernel FreeBSD** cuya principal característica es que se trata de un sistema operativo modular. Cada parte del código que se encarga de un servicio (protocolo) se ejecuta en un proceso diferente. Por ejemplo, en el caso de que exista un problema a nivel de software sólo dejará de funcionar esa parte, pero el resto se mantendrá estable.

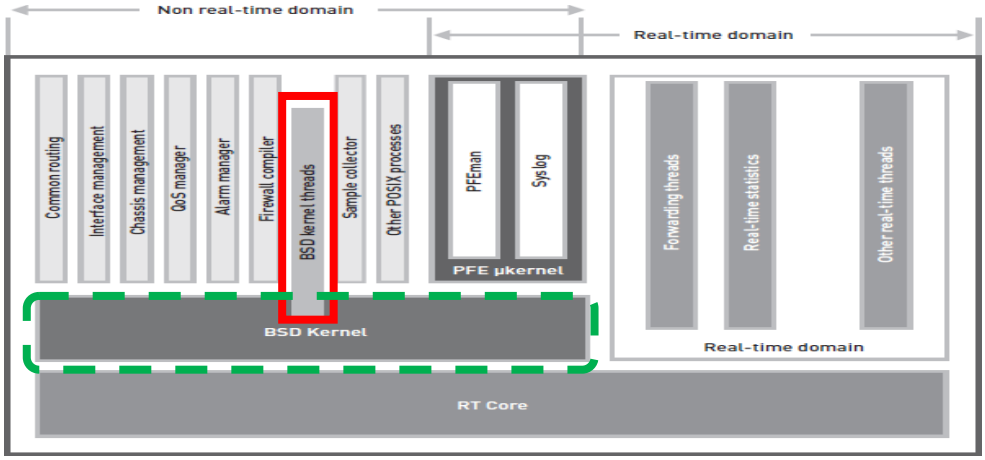


Figura 23: Arquitectura modular equipo NATBOX

3.2 Escenario pruebas

En este apartado definiremos además del entorno elegido para realizar el listado de pruebas, el proceso que debería seguir la petición de servicio que demande el usuario entre los equipos que conformen la maqueta de pruebas.

3.2.1 Arquitectura Red Móvil

A continuación reflejamos el escenario de la red móvil donde estableceremos una interconexión de equipos sobre los que se encaminará las peticiones de un flujo ficticio de peticiones de acceso de Internet.

Este escenario imitaría a uno real que provea el servicio de acceso a Internet con los equipos NATBOX, que junto con unas lógicas predefinidas, encaminarán las peticiones hacia la red externa.

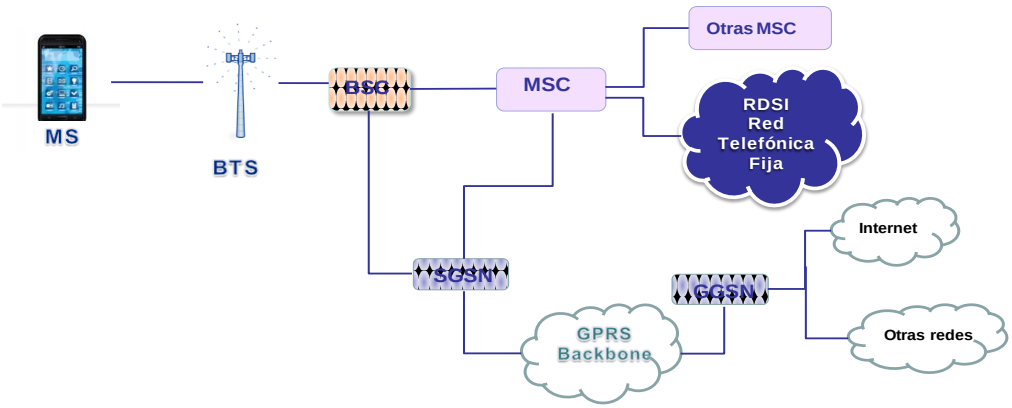


Figura 24: Red de Datos sobre la que establecer la maqueta de pruebas

El entorno dónde se realizarán las pruebas determinadas, se establecerá en el *core* de la red de paquetes de una red móvil tipo. Entendemos el *core*, como el núcleo de la arquitectura dónde se aplican las políticas de encaminamiento de las peticiones de acceso de usuarios recibidas desde la parte radio más externa de la arquitectura móvil. Tal y como aparece en la siguiente figura, en el Backbone sería el lugar dónde establecer el escenario de pruebas.

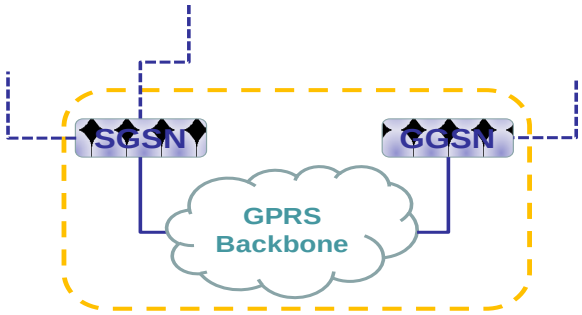


Figura 25: Núcleo de la red de datos

3.2.2 Maqueta pruebas

Posteriormente mostramos la arquitectura de la maqueta dónde se realizarán las pruebas. Detallaremos el lugar indicado del equipo **NATBOX** encargado de encaminar las peticiones de acceso al servicio que reclamen los usuarios de la red móvil, así como el proceso iniciado desde el terminal del usuario que requiere el acceso a Internet.

Para poder definir el escenario de pruebas es necesario realizar una serie de implementaciones y configuraciones en los equipos que van a formar parte del escenario de pruebas. Esas modificaciones se aplicarán en los equipos que en producción ofrecen el servicio de Internet sin escalarse en los equipos de **NATBOX**.

Algunos de los cambios a llevar a cabo en equipos que sostienen la red original serían estos:

- Modificar perfiles de Internet en equipos que necesitan autenticarse según políticas predefinidas del tipo de autenticación.

- Definir nuevas políticas de acceso en donde se describan las prioridades de uso de los equipos **NATBOX**.

- Especificar los puertos y direcciones IP de los equipos que formarán parte del escenario de pruebas.

- Estableceremos además distintas fases para poder establecer las contingencias necesarias entre varios equipos.

Todas estas modificaciones se llevarán a cabo en otros procesos del proyecto relacionado, es decir, que no formarán parte del objetivo principal.

Las configuraciones adecuadas se aplicarán en otras fases del proyecto.

3.2.3 Diseño inicial

Para comprender el flujo de la petición de acceso a Internet por parte de los usuarios, explicaremos brevemente cuál es el funcionamiento de los equipos que conforman el escenario de pruebas.

De entre todos los equipos que conforman el escenario, el equipo BBDD, conocido también como servidores tipo AAA o servidores Radius, gracias a su fiabilidad e interoperabilidad, integra un control de autenticación escalable y una potente gestión de usuarios que posee una configuración centralizada, convirtiéndolo en un servidor totalmente adaptativo.

Además de la base de datos, la arquitectura BBDD conforma una lógica de funciones alimentada por la información almacenada y relativa a los usuarios y sus funciones. Es decir, a través del MSISDN podemos averiguar qué usuarios deben realizar o no, funciones de traducción de direcciones (NAT).

A continuación mostraremos la arquitectura del piloto de pruebas que emplearemos para poder llevar a cabo las pruebas pertinentes necesarias para el desarrollo del proyecto.

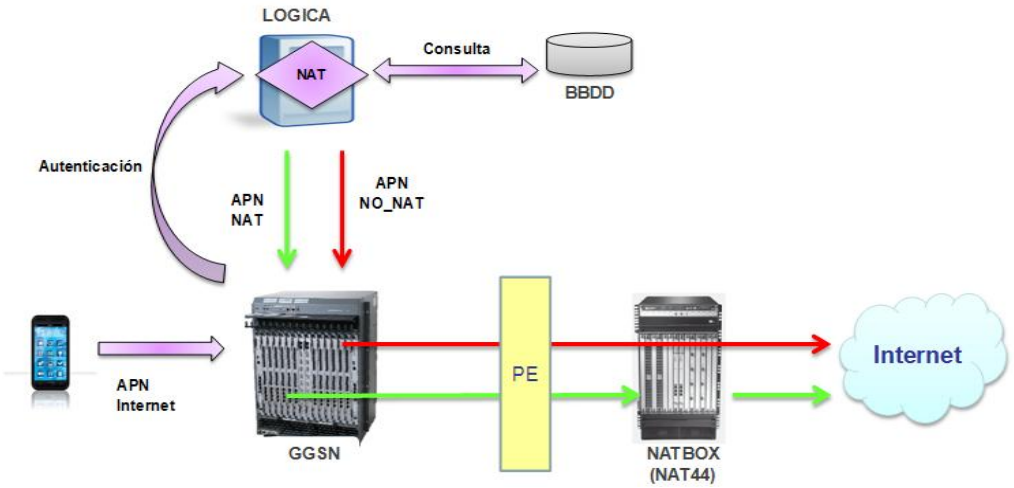


Figura 26: Núcleo de la red de datos

El flujo de la petición de acceso a Internet iniciada por el usuario desde su teléfono continúa las siguientes fases:

a. El usuario realiza una petición de acceso a internet a través de un apn (access point nework) de pruebas, configurado para probar el comportamiento del servicio requerido por el usuario determinado.

b. El equipo GGSN recibe esa petición y consulta el tipo de autenticación que debe aplicarse al usuario en concreto.

c. Posteriormente en el proceso de autenticación, los equipos basados en servidores Radius, a través de la consulta de la base de datos que almacena la información relativa a los usuarios (MSISDN, políticas de encaminamiento, reglas definidas…), asignarán un apn de salida para acceder a Internet.

d. Según esté definido en las bases de datos, el acceso de unos usuarios estarán configurados en un apn que deba encaminarse hacia el traductor **NATBOX**, algo que impedirá que todos los usuarios que requieran un acceso a Internet estén encaminados por el mismo canal.

e. Otros usuarios, por el contrario accederán a Internet directamente, con el apn de salida determinado desde el equipo GGSN hacia la red de Internet.

Es importante destacar que el equipo intermedio entre el GGSN y el NATBOX es un punto de acceso entre esos dos equipos, que también puede funcionar como acceso para otras redes que encaminen otros usuarios que necesiten acceder a Internet a través del NATBOX.

Así conseguimos que una única IP pública pueda emplearse por varios equipos con una IP privada. Por eso se definen grupos de direcciones IP públicas, conocidos como *pools* de Internet, que aplicarán la técnica de traducción para los usuarios que realicen peticiones de acceso a través del GGSN.

3.3 Pruebas Realizadas

En este punto, nos centraremos en comprobar si el comportamiento de la incursión del equipo **NATBOX** en la arquitectura de red móvil para resolver el problema del agotamiento de direcciones IP, es el esperado según los distintos servicios o aplicaciones requeridos por los usuarios.

3.3.1 Definición pruebas

Fundamentalmente definiremos las aplicaciones básicas cuyos accesos son requeridos, y veremos si con la arquitectura inicial establecida conseguimos acceder a esos servicios o si por el contrario deberíamos modificar o añadir nuevas plataformas, aplicar ciertas técnicas de acceso, o incluso redefinir la arquitectura propuesta.

Definiremos varios grupos de aplicaciones más comunes demandadas por los usuarios donde comprobaremos el impacto del equipo **NATBOX**. Después enfocaremos los protocolos sensibles a probar, y finalmente mostraremos en detalle un ejemplo de uno de los protocolos probados.

Seguidamente se detallan las aplicaciones y los protocolos empleados en estas pruebas de comunicación, junto con el objeto de la prueba a realizar:

APLICACIÓN	PROTOCOLO	TEST
Navegacion WEB	**HTTP**	Comprobar que pueden establecerse correctamente las conexiones en páginas populares de Internet: www.google.es, www.rae.es

Figura 27: Descripción prueba protocolo http

APLICACIÓN	PROTOCOLO	TEST
FTP	**FTP**	Comprobar que puede establecerse una conexión con un servidor ftp y que además pueden cargar y descargarse archivos sin que exista ningún error.

Figura 28: Descripción prueba protocolo ftp

APLICACIÓN	PROTOCOLO	TEST
E-mail	**POP3**	Comprobar que puede accederse a una cuenta de correo
	IMAP	Comprobar que puede accederse a una cuenta de correo

Figura 29: Descripción prueba aplicación email

APLICACIÓN	PROTOCOLO	TEST
P2P	**BitTorrent**	Comprobar que pueden realizarse descargas de archivos generando un BT desde un equipo ubicado tras el NAT y desde otro ubicado fuera del mismo

Figura 30: Descripción prueba aplicación P2P

APLICACIÓN	PROTOCOLO	TEST
Streaming	**youtube**	Comprobar que puede visualizarse los contenidos vídeo después de haber sido encaminados por el equipo NATBOX

Figura 31: Descripción prueba aplicación Streaming

APLICACIÓN	PROTOCOLO	TEST
VoIP	**Skype**	Comprobar que pueden realizarse y recibir llamadas, enviar y recibir mensajería instantánea, y establecer una videoconferencia.

Figura 32: Descripción prueba aplicación *Skype*

APLICACIÓN	PROTOCOLO	TEST
Otros	IPSec	Comprobar que puede establecerse correctamente un túnel IPSec a través del equipo que realiza NAT, utilizando ESP
	SSL	Comprobar que puede establecerse correctamente una conexión SSL

Figura 33: Descripción prueba otras aplicaciones

Cada una de estas pruebas se ha realizado de forma periódica durante varios días y en distintas franjas horarias para comprobar cómo afectan los lapsos de máxima y mínima actividad en cuanto a demanda de servicios por parte de los usuarios se refiere.

3.3.2 Desarrollo pruebas

En este apartado destacaremos el uso de un analizador de protocolos para poder revisar y confirmar el resultado de cada una de las pruebas que deseamos realizar. En este caso junto con el analizador *Wireshark* podemos reconstruir las sesiones de usuario que en su mayor parte provienen del protocolo TCP [25].

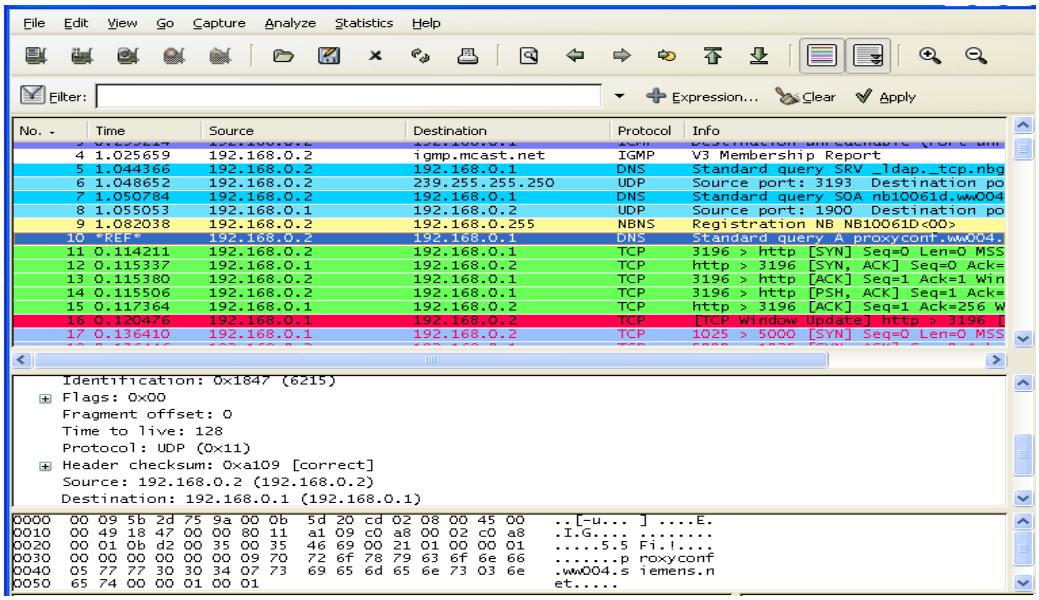


Figura 34: Aplicación Wireshark

Para poder capturar todas las tramas que se vean en el Interfaz de Internet, es necesaria una configuración en *modo promiscuo* de la herramienta analizadora. Un ordenador conectado a una red compartida captura todo el tráfico que circula por ella, así la información se transmite en una serie de paquetes con dirección física de quién lo envía y quién lo tiene que recibir. El fichero transmitido se divide en varios paquetes con tamaño predeterminado y el receptor es el único que captura los paquetes evaluando si lleva su dirección. Para el modo promiscuo una maquina intermedia captura todos los paquetes incluyendo paquetes destinados a él mismo y al resto de máquinas. Los nodos en ese modo copian los paquetes y luego vuelven a ponerlos en la red para que llegue al destinatario real.

Este modo resulta muy útil para ver cuál es la información que contienen los paquetes que atraviesan la red. Veremos a qué protocolos pertenecen, si están cifrados o no, o si la información se encuentra definida de forma clara. Concluiremos si la función de NAT se aplica correctamente o por el contrario encontramos problemas. De esta forma observaremos si el envío de paquetes entre el **NATBOX** y la salida a Internet es correcto.

A través de esta multiplataforma de análisis de red, seremos capaces de interpretar la información que aparece en los paquetes que se han enviado. Puesto que la captura es completa, deberemos aplicar filtros para poder obtener la información relevante de las trazas.

3.3.3 Resultado pruebas

Para cada uno de los protocolos a probar incluiremos capturas del tráfico generado en las peticiones de acceso a internet de un usuario, a través de la máquina de NATBOX.

Tendremos en cuenta que la **marca rosa**, corresponde con la dirección IP correspondiente al usuario, e indicaremos a qué corresponde cada **marca gris.**

3.3.3.1 Aplicación HTTP

A continuación mostraremos una captura de tráfico dónde se incluye el acceso a una página de internet, **www.rae.es**, a través de una primera petición a través del buscador de **www.google.es**. De esta forma mostraremos si esta petición finaliza satisfactoriamente en el entorno predefinido, así como los mensajes surgidos.

Marcamos la entrada GET que solicita al servidor de *google* (marca **gris**), la pagina a la que deseamos acceder.

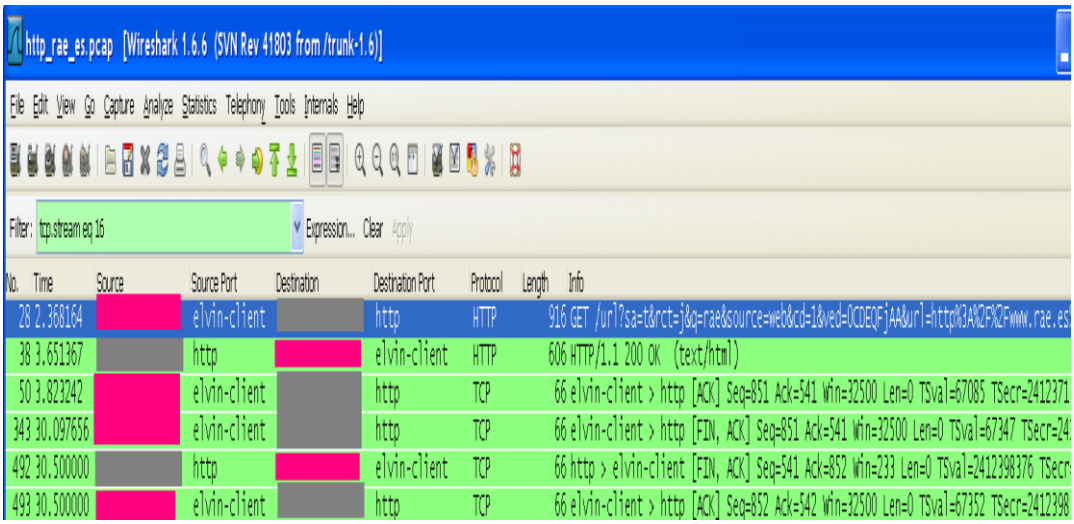


Figura 35: Trama mensaje GET

Mostramos también los datos correspondientes con la traza señalada.

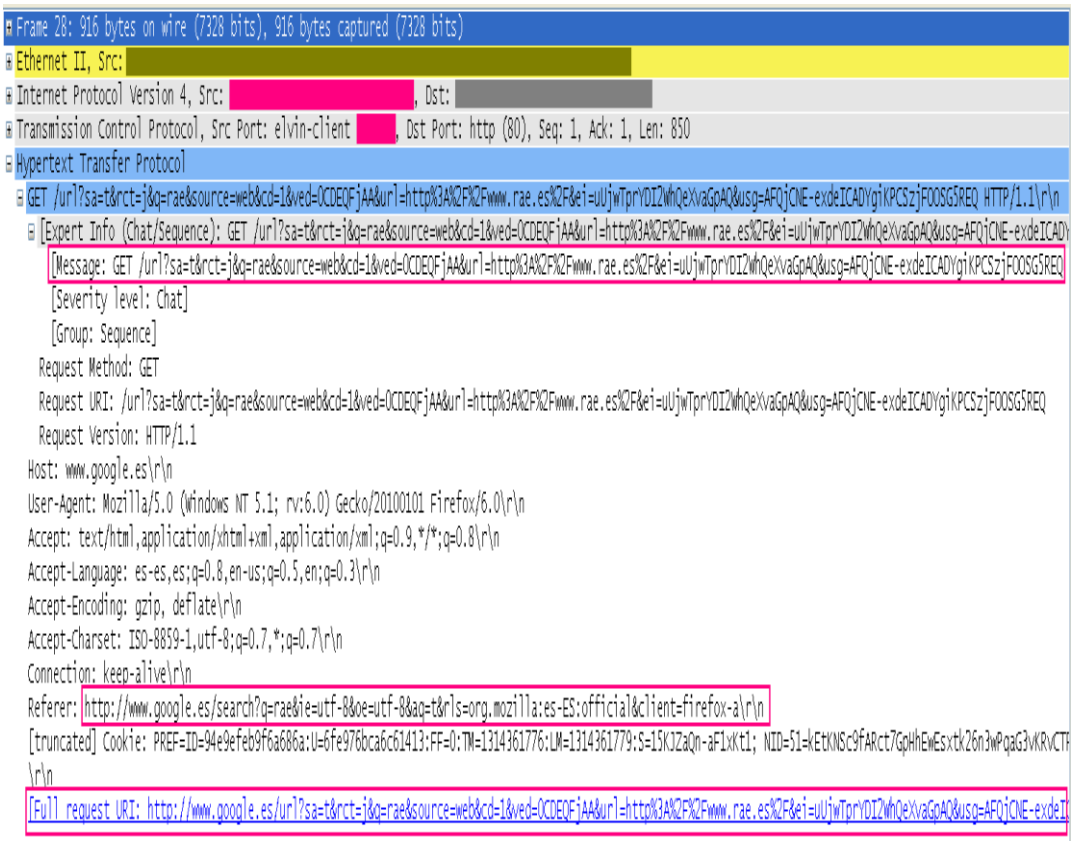


Figura 36: Trama mensaje GET detalles

Tal y como se muestra en la traza, aparece un aviso de que existe un aviso en la capa de nivel 2, que hace referencia a los paquetes enviados. Básicamente nos indica que existe un desbordamiento de paquetes desde la fuente, en este caso, peticiones del usuario hacia el acceso a Internet. Desplegamos para ver el contenido del mensaje de aviso:

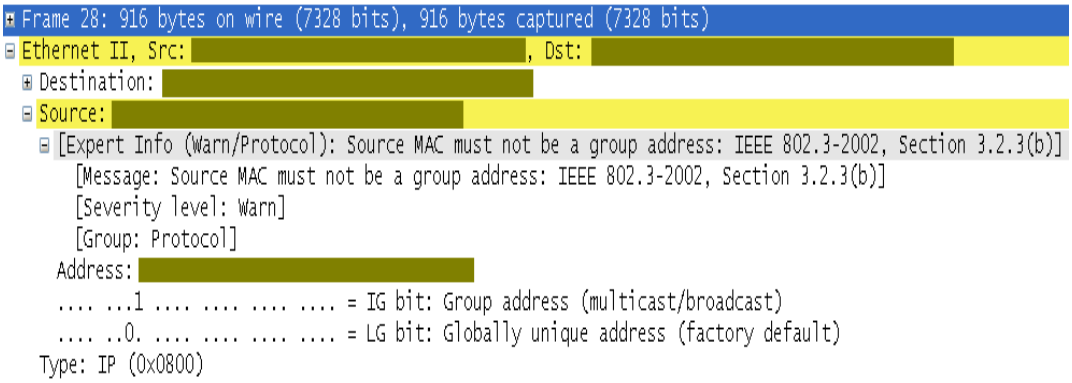


Figura 37: Detalles mensaje con avisos

Mostramos la traza relacionada con la respuesta correcta de la petición de acceso a *google* anterior:

Figura 38: Trama mensaje código 200 mensaje Http

En la siguiente captura mostramos el flujo de todos los ACKs que indican que la sesión TCP abierta para acceder al servicio de google se ha establecido sin problemas.

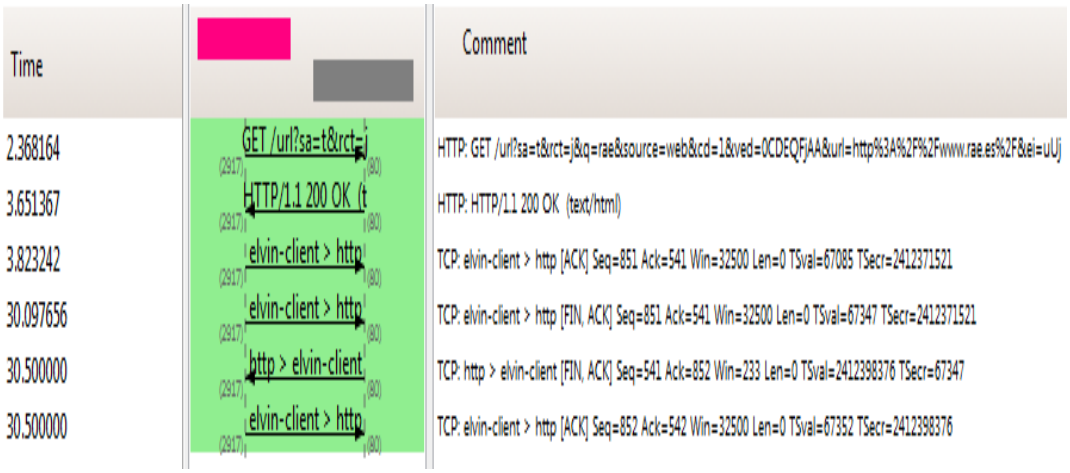


Figura 39: Flujo mensajes establecimiento sesión http

Para poder acceder a la dirección electrónica www.rae.es, y navegar por los distintos elementos de la página, el proceso es exactamente el mismo. A través del método GET del protocolo HTTP se van realizando peticiones a los servidores que contienen la información requerida. El proceso global ha tenido varias peticiones que presentamos a continuación:

Topic / Item	Count
HTTP Requests by HTTP Host	13
www.google.es	1
/url?sa=t&rct=j&q=rae&source=web&cd=1&ved=0CDEQFjAA&url=http%3A%2F%2Fwww.rae.es%2F&ei=uUjwTprYDI2WhQeXvaGpAQ&usg=AFQjCNE-exdeICADYgjKPCSzjFOOSG5REQ	1
www.rae.es	12
/	1
/rae.html	1
/style.css	1
/Imagenes/graficos.nsf/recursos/CSS*general_text/$File/general_text.css	1
/images/logotop.png	1
/images/Estudiante3D.png	1
/images/image002.gif	1
/images/iconRtArrow_20x20.gif	1
/images/panhis.gif	1
/images/fonetica3d.png	1
/images/escRAE4.png	1
/favicon.ico	1

Figura 40: Peticiones globales acceso servicios http

En esta gráfica se muestra la evolución del tráfico generado durante el tiempo que se ha mantenido la captura del analizador de *Wireshark*.

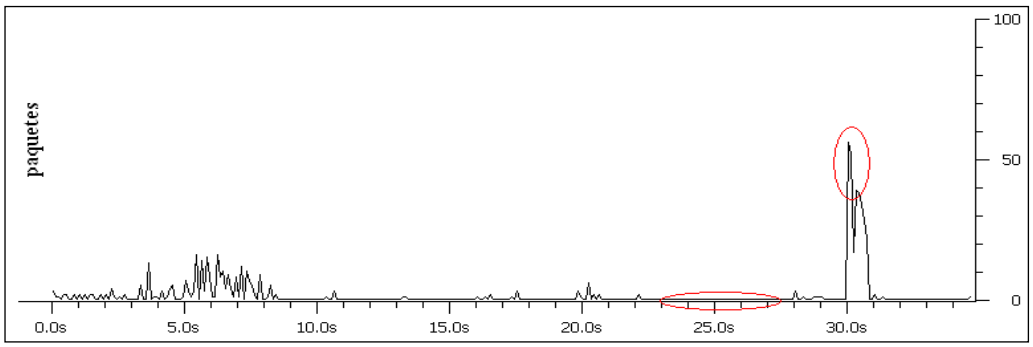


Figura 41: Evolución tráfico durante las sesiones http establecidas

Tal y como aparece reflejado en la gráfica, el tráfico generado en esta sesión posee bastantes valles correspondientes con errores en el envío y recepción de paquetes tipo HTTP, y un solo valor máximo, perteneciente a la petición de acceso a la página de www.rae.es y la navegación apropiada.

En este flujo de datos, donde existen no solo, peticiones exitosas, aparecen varias que contienen ciertos errores a tener en cuenta para las posteriores conclusiones. Algunos de estos ejemplos con errores son los siguientes:

En este caso comprobamos el código 302 de la respuesta al método GET que nos indica que los datos requeridos al servidor se encuentran en otro servidor, por lo que deberían volver a establecerse otras sesiones HTTP para poder encontrar el servicio requerido.

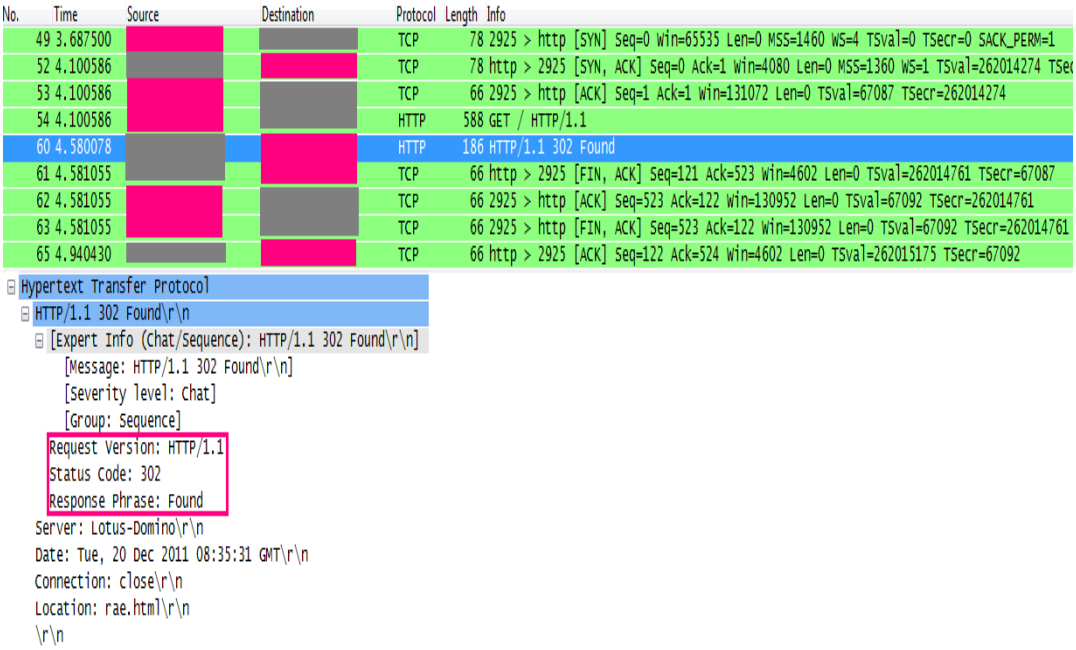


Figura 42: Trama mensaje código 302 mensaje Http

Las capturas siguientes muestran problemas detectados en la transmisión de paquetes que se producen en las sesiones TCP y que están codificados con varios valores.

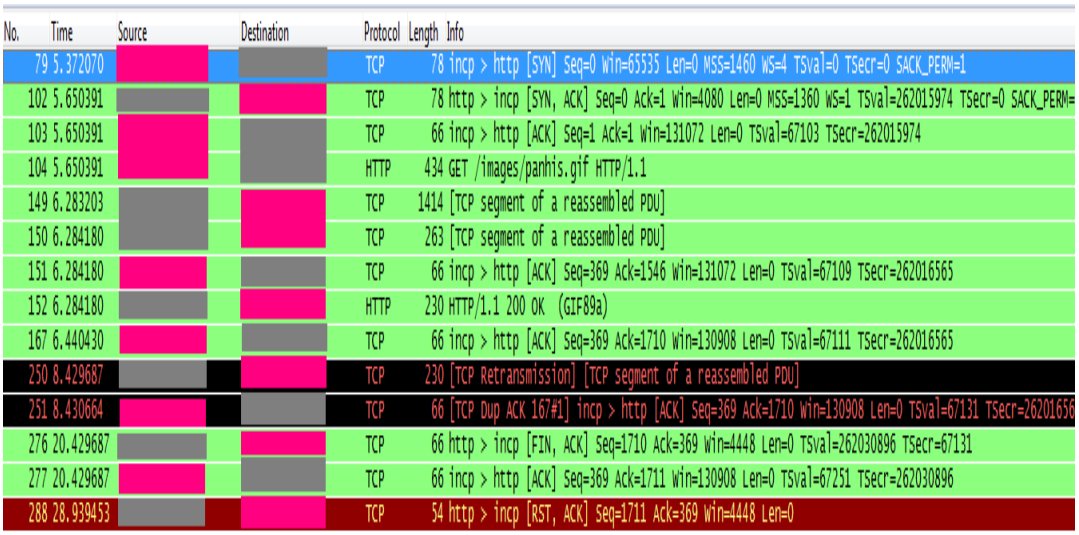


Figura 43: Problemas detectados en la transmisión de paquetes http

i. TCP Retransmission

Tal y como se representa en la captura, entre las trazas TCP que se envían, se requiere una trama de tipo ACK que confirme que el paquete enviado en la trama 152 ha llegado con éxito. Esta retransmisión se produce porque no obtiene esa confirmación y vuelve a enviar la misma trama reclamando esa confirmación.

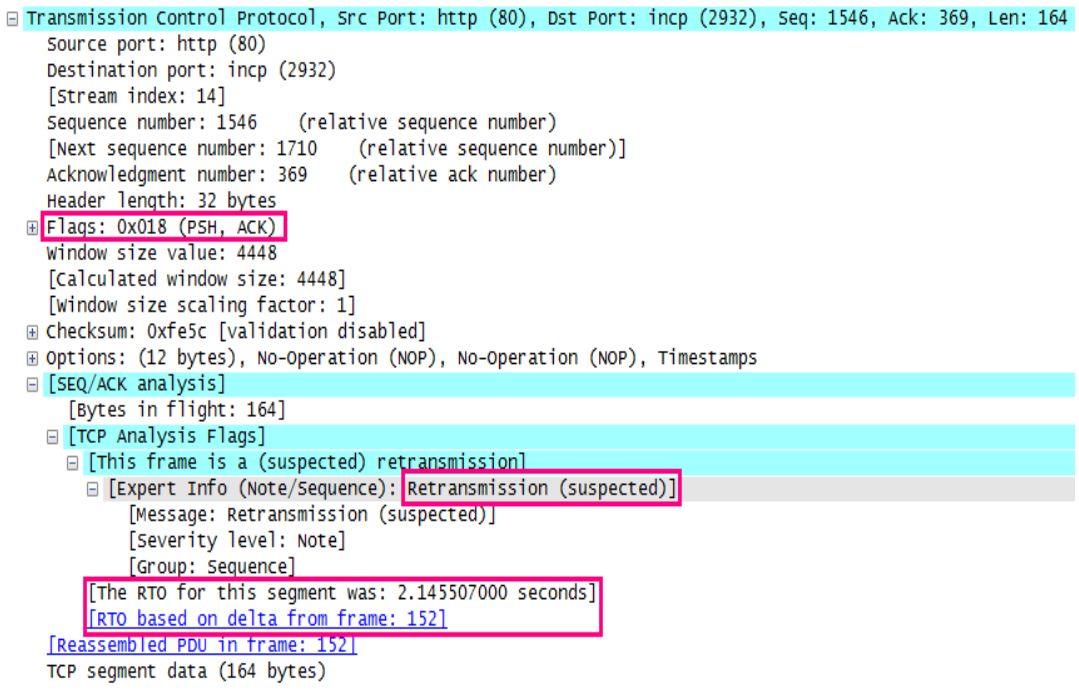


Figura 44: Detalles trama Retransmission

ii. TCP Duplicated ACK

En este caso, se trata de un ACK duplicado que debe reenviarse de nuevo, para poder confirmar la trama que se ha retransmitido en la captura anterior, y que en tramas de orden anterior ya se envió.

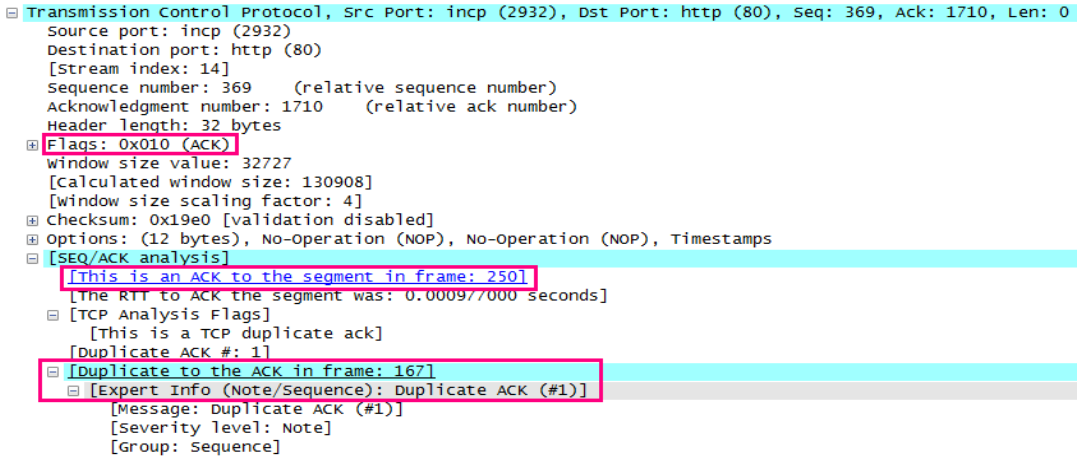


Figura 45: Detalles trama Duplicated ACK

iii. Connection RESET

En este caso, comprobamos que se envía una trama con los *flags* RST y ACK activados. Algunos de los posibles errores podrían ser:

- Envío RST en respuestas a la recepción de un paquete de socket cerrado.
- Difícil encontrar una la causa de este error, pero podría ser para bloquear el tráfico determinado en ese puerto.
- El comportamiento de NAT que genera una plaga de errores RST
- Envío forzado de este tipo de mensajes cada cierto tiempo.

Son algunas de las causas por las que pueden surgir con este tipo de tramas recibidas, pero que no pueden concluirse que sea ésta la razón del envío de esta trama.

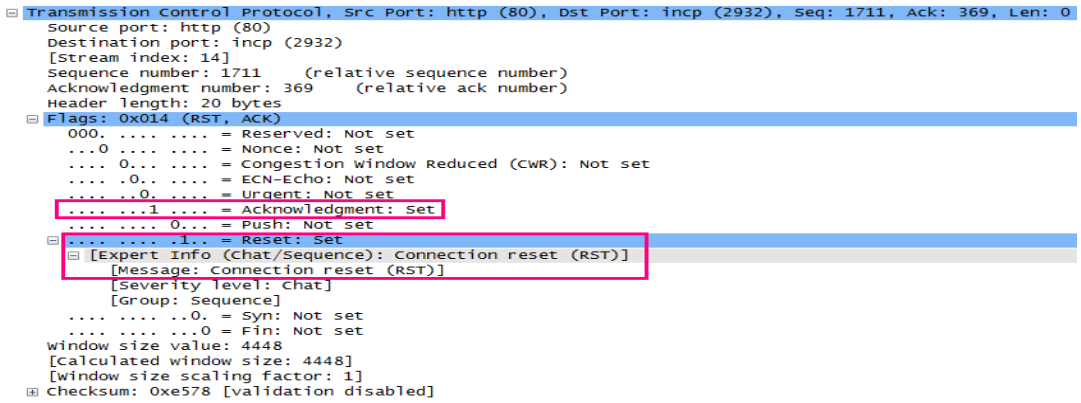


Figura 46: Detalles trama Connection Reset

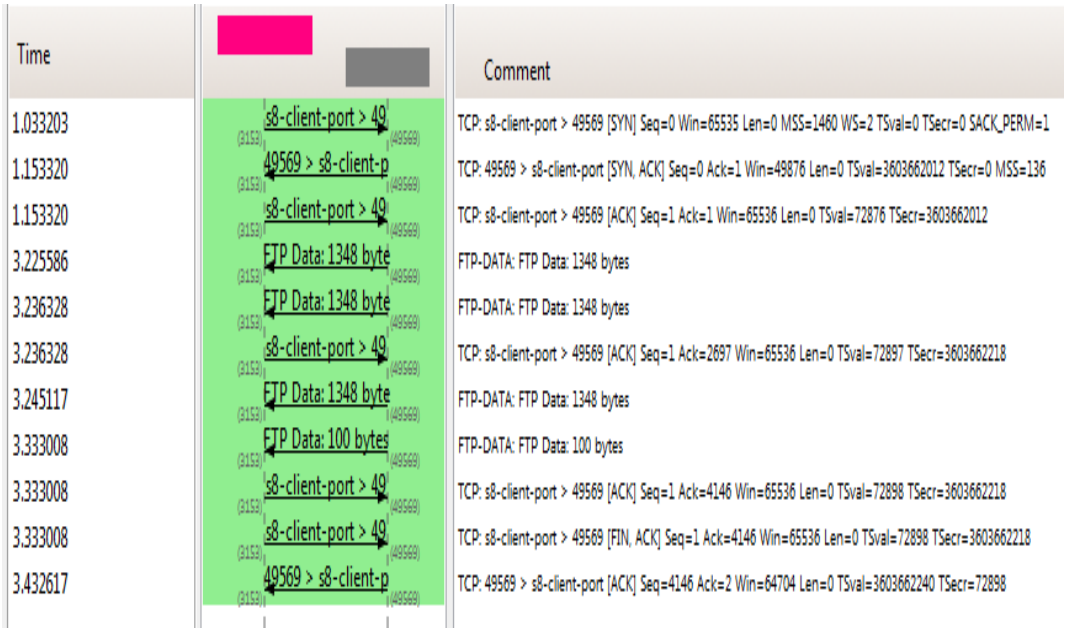
3.3.3.2 Aplicación FTP

La siguiente captura muestra el establecimiento de una conexión con un servidor ftp en la que existe un intercambio de carga y descarga de archivos.

En esta primera traza comprobamos como se establece la sesión FTP en **modo activo**, entre el usuario y el servidor FTP, **marca gris**. El flujo de este establecimiento se representa a continuación:

Figura 47: Flujo trazas establecimiento sesión ftp

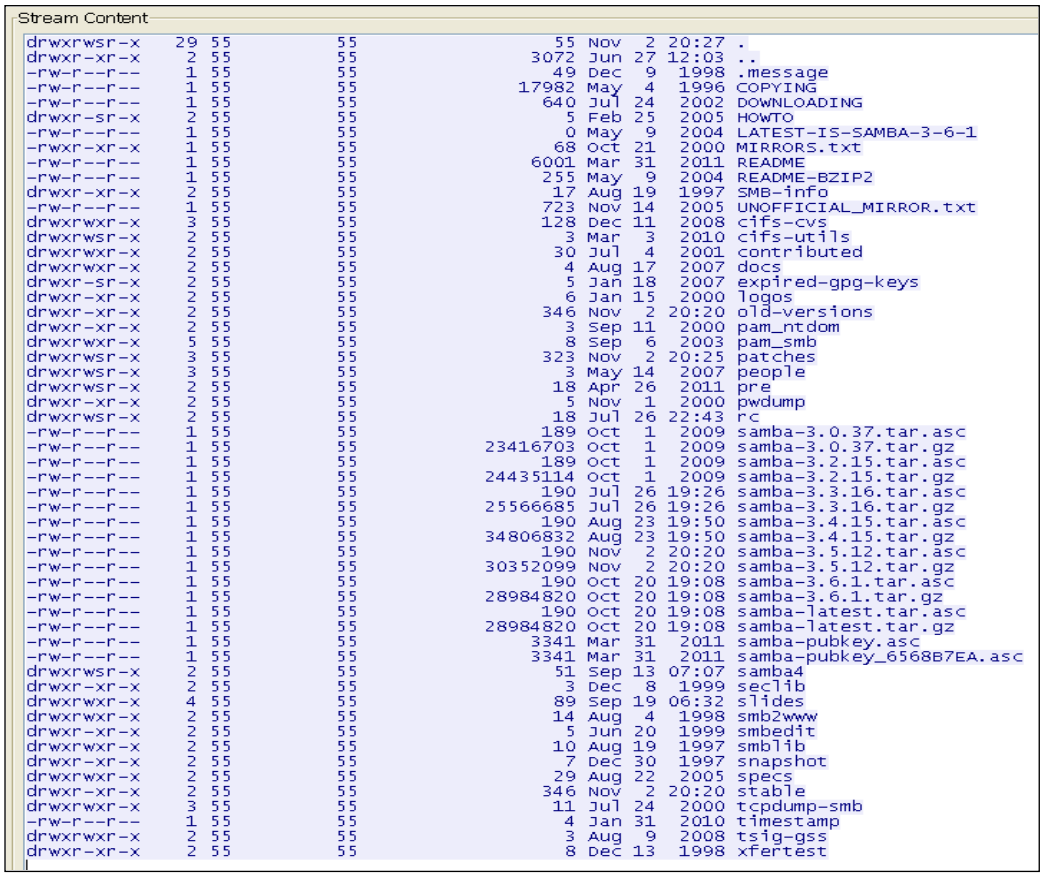
En la siguiente traza, establecida la sesión en **modo pasivo**, observamos los siguientes detalles de carga y descarga de archivos:



Time		Comment
1.033203	s8-client-port > 49	TCP: s8-client-port > 49569 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 TSval=0 TSecr=0 SACK_PERM=1
1.153320	49569 > s8-client-p	TCP: 49569 > s8-client-port [SYN, ACK] Seq=0 Ack=1 Win=49876 Len=0 TSval=3603662012 TSecr=0 MSS=136
1.153320	s8-client-port > 49	TCP: s8-client-port > 49569 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=72876 TSecr=3603662012
3.225586	FTP Data: 1348 byte	FTP-DATA: FTP Data: 1348 bytes
3.236328	FTP Data: 1348 byte	FTP-DATA: FTP Data: 1348 bytes
3.236328	s8-client-port > 49	TCP: s8-client-port > 49569 [ACK] Seq=1 Ack=2697 Win=65536 Len=0 TSval=72897 TSecr=3603662218
3.245117	FTP Data: 1348 byte	FTP-DATA: FTP Data: 1348 bytes
3.333008	FTP Data: 100 bytes	FTP-DATA: FTP Data: 100 bytes
3.333008	s8-client-port > 49	TCP: s8-client-port > 49569 [ACK] Seq=1 Ack=4146 Win=65536 Len=0 TSval=72898 TSecr=3603662218
3.333008	s8-client-port > 49	TCP: s8-client-port > 49569 [FIN, ACK] Seq=1 Ack=4146 Win=65536 Len=0 TSval=72898 TSecr=3603662218
3.432617	49569 > s8-client-p	TCP: 49569 > s8-client-port [ACK] Seq=4146 Ack=2 Win=64704 Len=0 TSval=3603662240 TSecr=72898

Figura 48: Trazas descarga de archivos en la sesión ftp

A través de la herramienta *Wireshark*, comprobamos los datos descargados en esta sesión:



Stream Content

```
drwxrwsr-x   29 55         55              55 Nov  2 20:27 .
drwxr-xr-x    2 55         55            3072 Jun 27 12:03 ..
-rw-r--r--    1 55         55              49 Dec  9  1998 .message
-rw-r--r--    1 55         55           17982 May  4  1996 COPYING
-rw-r--r--    1 55         55             640 Jul 24  2002 DOWNLOADING
drwxr-sr-x    2 55         55               5 Feb 25  2005 HOWTO
-rw-r--r--    1 55         55               0 May  9  2004 LATEST-IS-SAMBA-3-6-1
-rwxr-xr-x    1 55         55              68 Oct 21  2000 MIRRORS.txt
-rw-r--r--    1 55         55            6001 Mar 31  2011 README
-rw-r--r--    1 55         55             255 May  9  2004 README-BZIP2
drwxr-xr-x    2 55         55              17 Aug 19  1997 SMB-info
-rw-r--r--    1 55         55             723 Nov 14  2005 UNOFFICIAL_MIRROR.txt
drwxrwxr-x    3 55         55             128 Dec 11  2008 cifs-cvs
drwxrwsr-x    2 55         55               3 Mar  3  2010 cifs-utils
drwxrwxr-x    2 55         55              30 Jul  4  2001 contributed
drwxrwxr-x    2 55         55               4 Aug 17  2007 docs
drwxr-sr-x    2 55         55               5 Jan 18  2007 expired-gpg-keys
drwxr-xr-x    2 55         55               6 Jan 15  2000 logos
drwxr-xr-x    2 55         55             346 Nov  2 20:20 old-versions
drwxr-xr-x    2 55         55               3 Sep 11  2000 pam_ntdom
drwxrwxr-x    5 55         55               8 Sep  6  2003 pam_smb
drwxrwsr-x    3 55         55             323 Nov  2 20:25 patches
drwxrwsr-x    3 55         55               3 May 14  2007 people
drwxrwsr-x    2 55         55              18 Apr 26  2011 pre
drwxr-xr-x    2 55         55               5 Nov  1  2000 pwdump
drwxrwsr-x    2 55         55              18 Jul 26 22:43 rc
-rw-r--r--    1 55         55             189 Oct  1  2009 samba-3.0.37.tar.asc
-rw-r--r--    1 55         55        23416703 Oct  1  2009 samba-3.0.37.tar.gz
-rw-r--r--    1 55         55             189 Oct  1  2009 samba-3.2.15.tar.asc
-rw-r--r--    1 55         55        24435114 Oct  1  2009 samba-3.2.15.tar.gz
-rw-r--r--    1 55         55             190 Jul 26 19:26 samba-3.3.16.tar.asc
-rw-r--r--    1 55         55        25566685 Jul 26 19:26 samba-3.3.16.tar.gz
-rw-r--r--    1 55         55             190 Aug 23 19:50 samba-3.4.15.tar.asc
-rw-r--r--    1 55         55        34806832 Aug 23 19:50 samba-3.4.15.tar.gz
-rw-r--r--    1 55         55             190 Nov  2 20:20 samba-3.5.12.tar.asc
-rw-r--r--    1 55         55        30352099 Nov  2 20:20 samba-3.5.12.tar.gz
-rw-r--r--    1 55         55             190 Oct 20 19:08 samba-3.6.1.tar.asc
-rw-r--r--    1 55         55        28984820 Oct 20 19:08 samba-3.6.1.tar.gz
-rw-r--r--    1 55         55             190 Oct 20 19:08 samba-latest.tar.asc
-rw-r--r--    1 55         55        28984820 Oct 20 19:08 samba-latest.tar.gz
-rw-r--r--    1 55         55            3341 Mar 31  2011 samba-pubkey.asc
-rw-r--r--    1 55         55            3341 Mar 31  2011 samba-pubkey_6568B7EA.asc
drwxrwsr-x    2 55         55              51 Sep 13 07:07 samba4
drwxr-xr-x    2 55         55               3 Dec  8  1999 seclib
drwxrwxr-x    4 55         55              89 Sep 19 06:32 slides
drwxrwxr-x    2 55         55              14 Aug  4  1998 smb2www
drwxr-xr-x    2 55         55               5 Jun 20  1999 smbedit
drwxrwxr-x    2 55         55              10 Aug 19  1997 smblib
drwxr-xr-x    2 55         55               7 Dec 30  1997 snapshot
drwxrwxr-x    2 55         55              29 Aug 22  2005 specs
drwxr-xr-x    2 55         55             346 Nov  2 20:20 stable
drwxrwxr-x    3 55         55              11 Jul 24  2000 tcpdump-smb
-rw-r--r--    1 55         55               4 Jan 31  2010 timestamp
drwxrwxr-x    2 55         55               3 Aug  9  2008 tsig-gss
drwxr-xr-x    2 55         55               8 Dec 13  1998 xfertest
```

Figura 49: Información descargada durante la sesión ftp establecida

Además de errores relacionados con las trazas correspondientes con el protocolo TCP, queremos destacar uno de los errores que hemos observado.

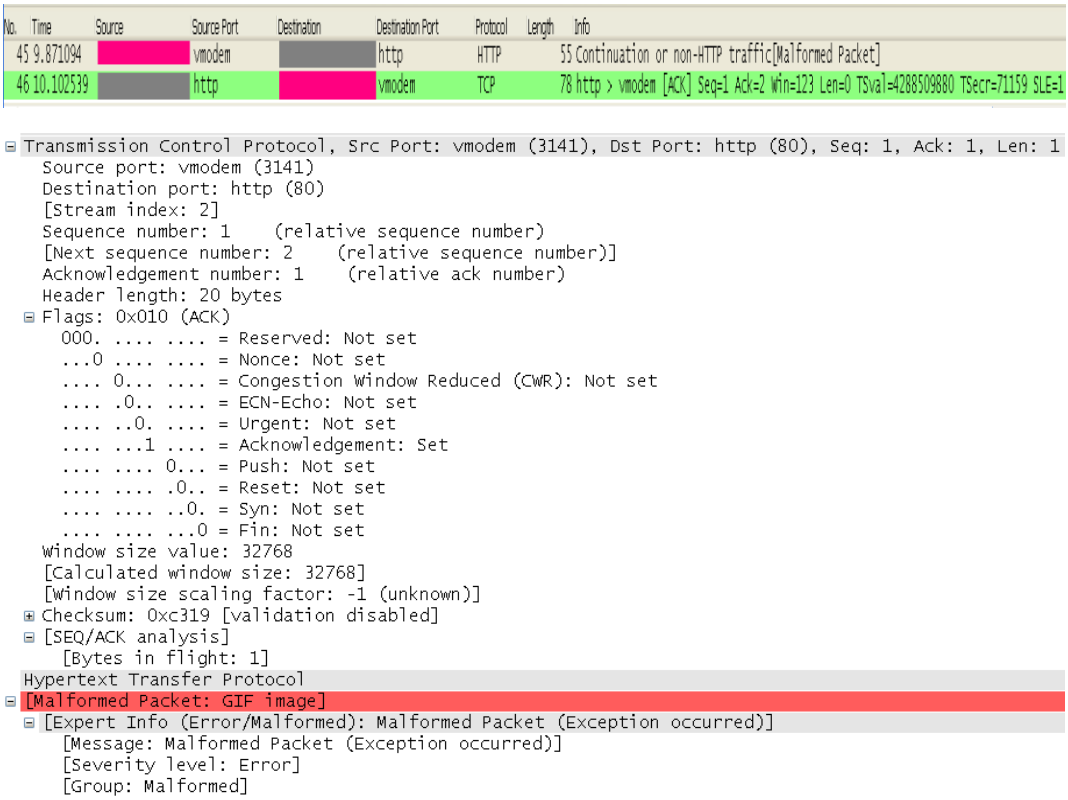


Figura 50: Problema detectado en la sesión ftp

A continuación mostraremos la grafica donde comprobamos globalmente como es el comportamiento de una sesión FTP:

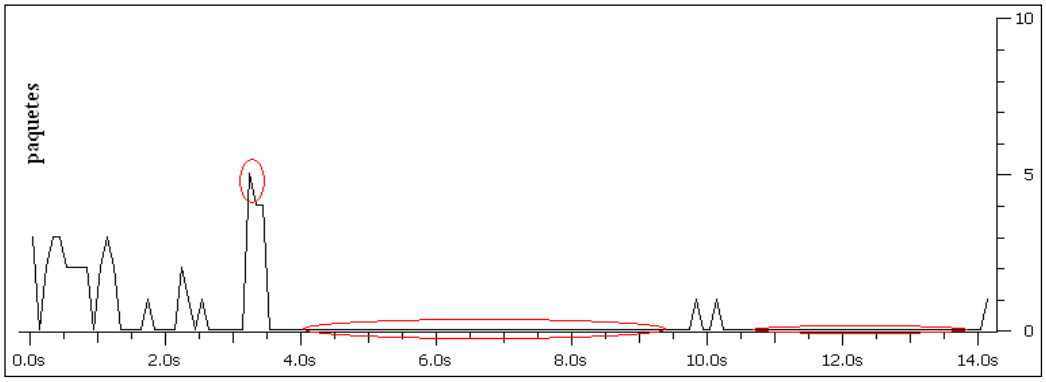


Figura 51: Evolución tráfico durante la sesión ftp establecida

El tráfico que podemos tener en una sesión ftp ya sea en modo activo o pasivo, muestra un comportamiento en los que solo en momentos puntuales encontramos descarga de paquetes. Principalmente se basa en mensajes de establecimiento y control de sesiones en los que no existe gran parte de volumen de tráfico.

3.3.3.3 Aplicación Email

3.3.3.2.1. POP3

En este caso, mostramos como acceder a una cuenta de correo electrónico a través del protocolo POP3:

Previamente a mostrar el intercambio de trazas que se sucede con la aplicación POP3, mostraremos que hemos accedido al servidor de correo a través de *google.* Así es necesario mostrar el sistema de resolución de nombres DNS que nos ofrece el camino para acceder al servidor, **marca gris**.

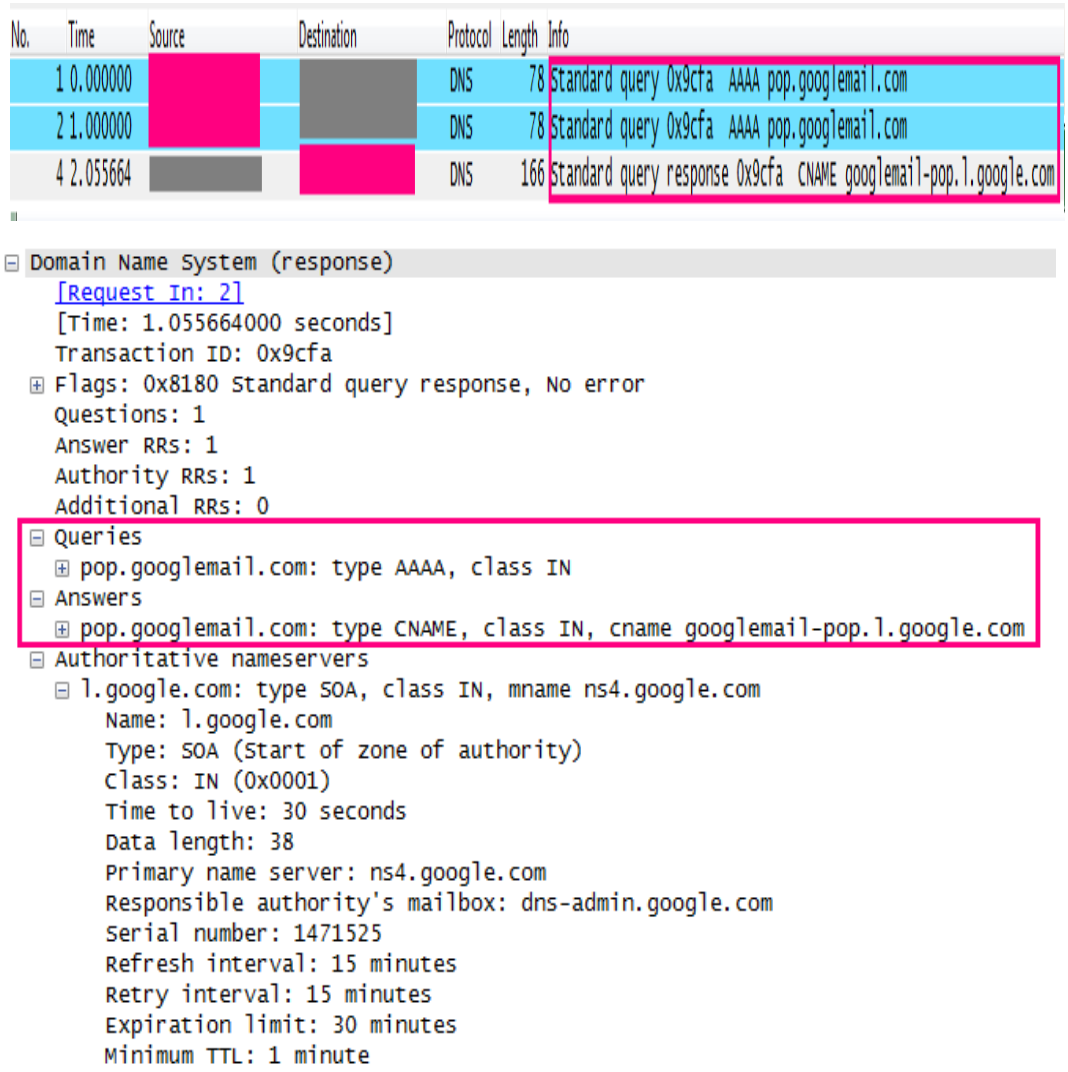
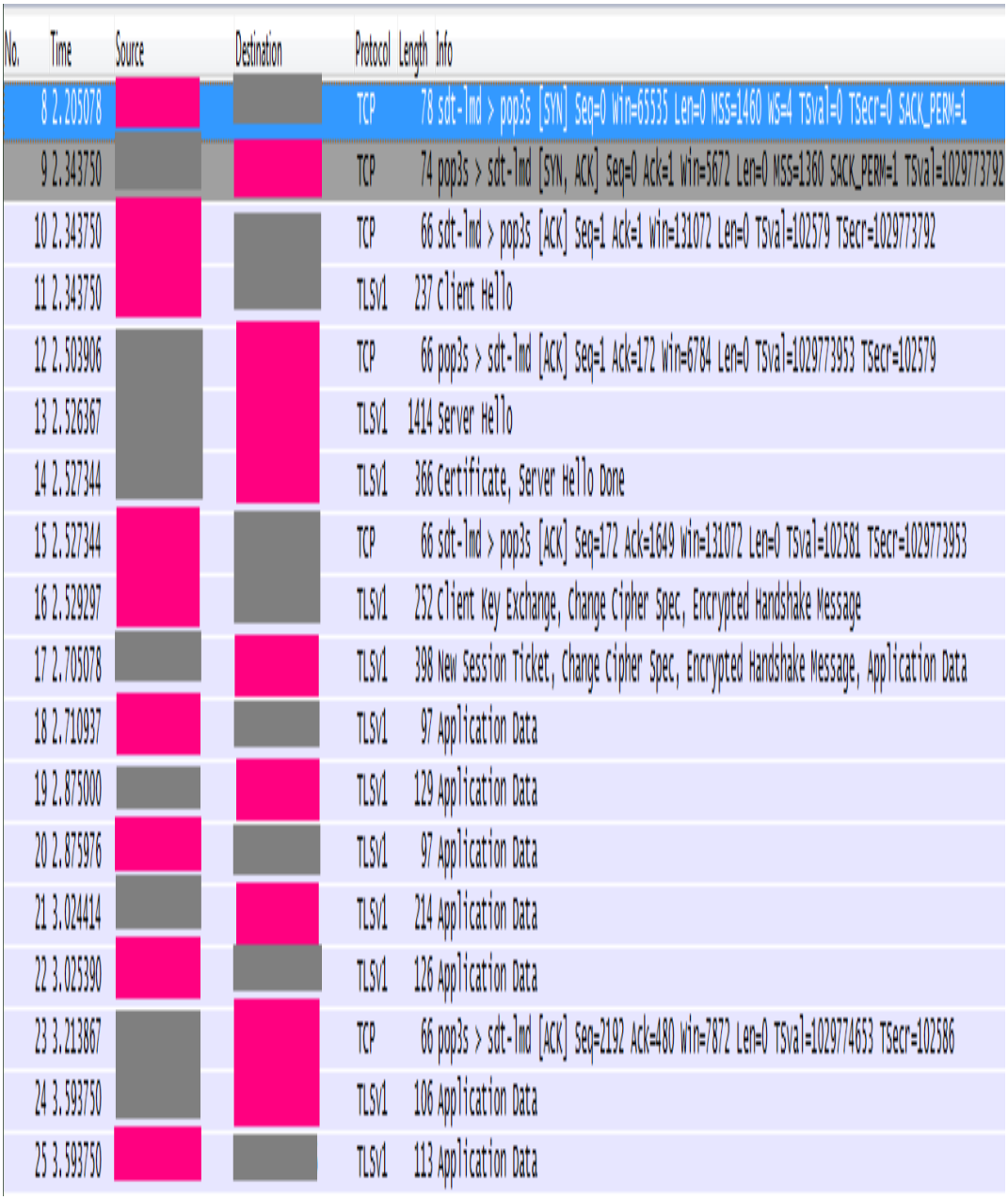


Figura 52: Petición acceso al servidor *google*

El establecimiento de una sesión POP3 es el siguiente:



No.	Time	Source	Destination	Protocol	Length	Info
8	2.205078	[redacted]	[redacted]	TCP	78	sdt-lmd > pop3s [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 TSval=0 TSecr=0 SACK_PERM=1
9	2.343750	[redacted]	[redacted]	TCP	74	pop3s > sdt-lmd [SYN, ACK] Seq=0 Ack=1 Win=5672 Len=0 MSS=1360 SACK_PERM=1 TSval=1029773792
10	2.343750	[redacted]	[redacted]	TCP	66	sdt-lmd > pop3s [ACK] Seq=1 Ack=1 Win=131072 Len=0 TSval=102579 TSecr=1029773792
11	2.343750	[redacted]	[redacted]	TLSv1	237	Client Hello
12	2.503906	[redacted]	[redacted]	TCP	66	pop3s > sdt-lmd [ACK] Seq=1 Ack=172 Win=6784 Len=0 TSval=1029773953 TSecr=102579
13	2.526367	[redacted]	[redacted]	TLSv1	1414	Server Hello
14	2.527344	[redacted]	[redacted]	TLSv1	366	Certificate, Server Hello Done
15	2.527344	[redacted]	[redacted]	TCP	66	sdt-lmd > pop3s [ACK] Seq=172 Ack=1649 Win=131072 Len=0 TSval=102581 TSecr=1029773953
16	2.529297	[redacted]	[redacted]	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
17	2.705078	[redacted]	[redacted]	TLSv1	398	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message, Application Data
18	2.710937	[redacted]	[redacted]	TLSv1	97	Application Data
19	2.875000	[redacted]	[redacted]	TLSv1	129	Application Data
20	2.875976	[redacted]	[redacted]	TLSv1	97	Application Data
21	3.024414	[redacted]	[redacted]	TLSv1	214	Application Data
22	3.025390	[redacted]	[redacted]	TLSv1	126	Application Data
23	3.213867	[redacted]	[redacted]	TCP	66	pop3s > sdt-lmd [ACK] Seq=2192 Ack=480 Win=7872 Len=0 TSval=1029774653 TSecr=102586
24	3.593750	[redacted]	[redacted]	TLSv1	106	Application Data
25	3.593750	[redacted]	[redacted]	TLSv1	113	Application Data

Figura 53: Establecimiento sesión POP3

A continuación mostramos el flujo de trazas que aparecen en la traza anterior, y que nos ofrece una mayor visibilidad del comportamiento de esta aplicación de correo electrónico:

Figura 54: Inicio Establecimiento flujo de trazas sesión POP3

Podemos comprobar que existe un protocolo TLS que se utiliza para la autenticación del usuario en determinadas aplicaciones que lo requieran. Esta aplicación la estudiaremos en posteriores subíndices. Para este apartado solo trataremos las aplicaciones de correo.

Puesto que en este tipo de aplicaciones existen bastantes mensajes entre los servidores de correo y el cliente, la traza anterior la cortamos para luego mostrar cual sería el fin de la sesión de correo electrónico:

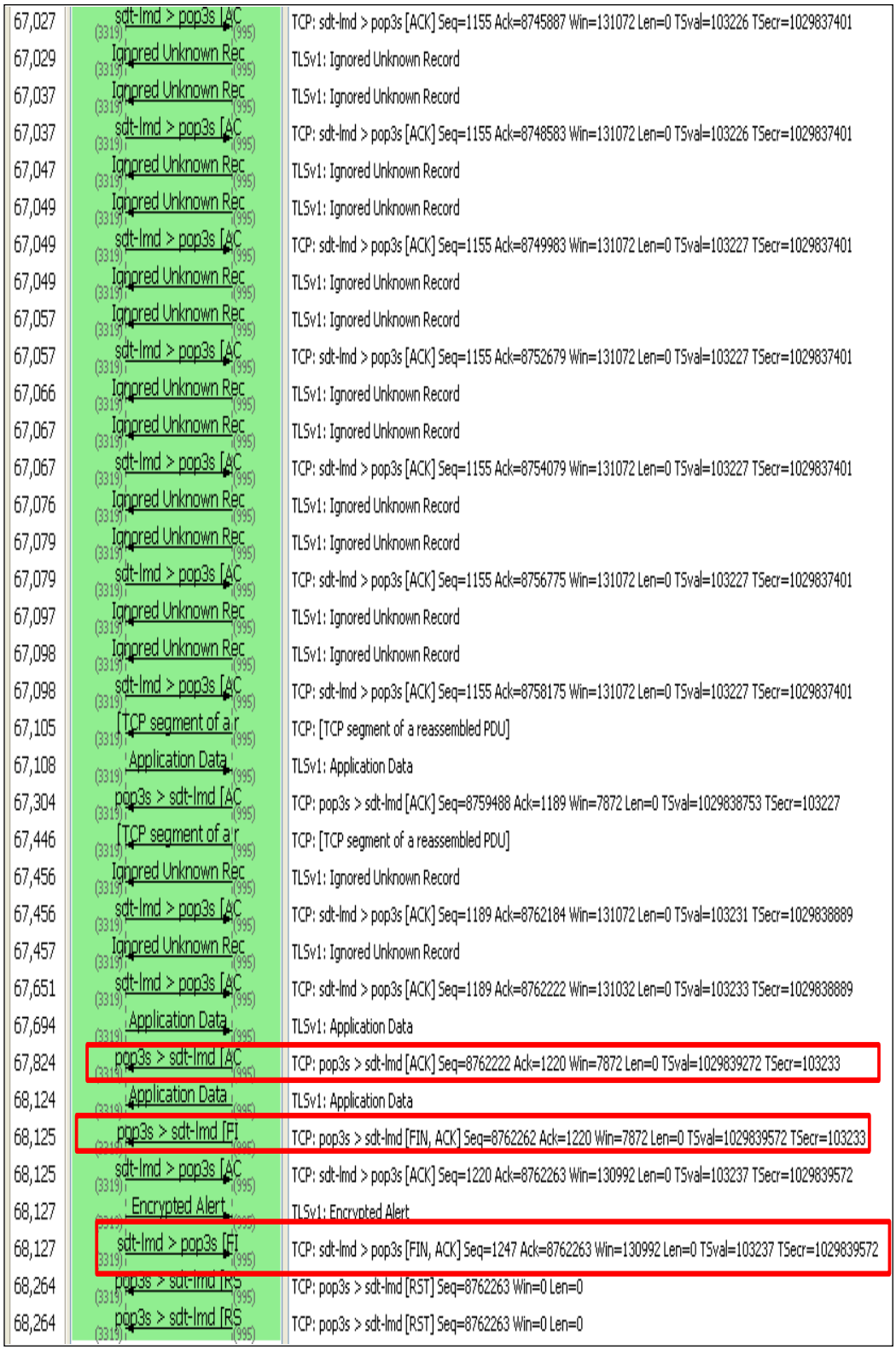
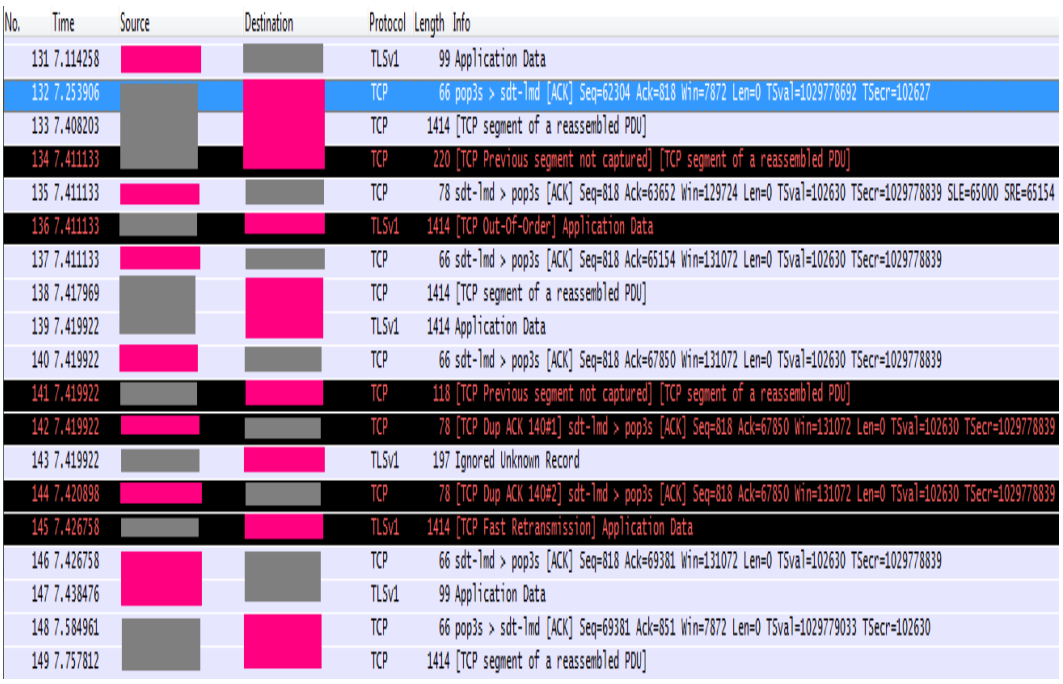


Figura 55: Fin Establecimiento flujo de trazas sesión POP3

Como hemos comentado anteriormente, mostraremos cuales son los errores con los que nos hemos ido encontrando en las pruebas relacionadas con esta aplicación:

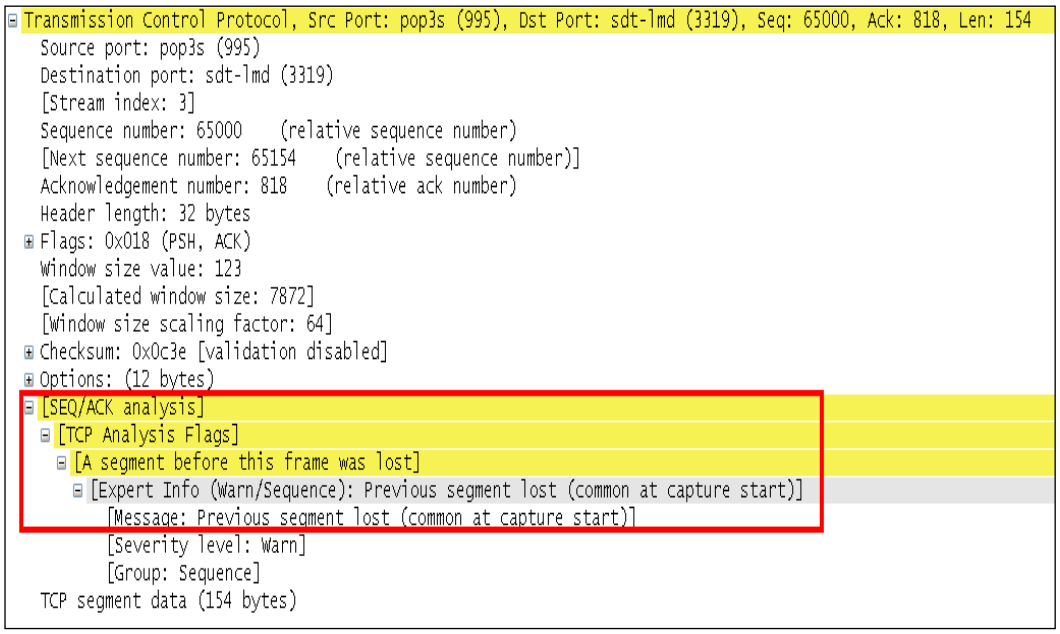


No.	Time	Source	Destination	Protocol	Length	Info
131	7.114258	[redacted]	[redacted]	TLSv1	99	Application Data
132	7.253906	[redacted]	[redacted]	TCP	66	pop3s > sdt-lmd [ACK] Seq=62304 Ack=818 Win=7872 Len=0 TSval=1029778692 TSecr=102627
133	7.408203	[redacted]	[redacted]	TCP	1414	[TCP segment of a reassembled PDU]
134	7.411133	[redacted]	[redacted]	TCP	220	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
135	7.411133	[redacted]	[redacted]	TCP	78	sdt-lmd > pop3s [ACK] Seq=818 Ack=63652 Win=129724 Len=0 TSval=102630 TSecr=1029778839 SLE=65000 SRE=65154
136	7.411133	[redacted]	[redacted]	TLSv1	1414	[TCP Out-Of-Order] Application Data
137	7.411133	[redacted]	[redacted]	TCP	66	sdt-lmd > pop3s [ACK] Seq=818 Ack=65154 Win=131072 Len=0 TSval=102630 TSecr=1029778839
138	7.417969	[redacted]	[redacted]	TCP	1414	[TCP segment of a reassembled PDU]
139	7.419922	[redacted]	[redacted]	TLSv1	1414	Application Data
140	7.419922	[redacted]	[redacted]	TCP	66	sdt-lmd > pop3s [ACK] Seq=818 Ack=67850 Win=131072 Len=0 TSval=102630 TSecr=1029778839
141	7.419922	[redacted]	[redacted]	TCP	118	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
142	7.419922	[redacted]	[redacted]	TCP	78	[TCP Dup ACK 140#1] sdt-lmd > pop3s [ACK] Seq=818 Ack=67850 Win=131072 Len=0 TSval=102630 TSecr=1029778839
143	7.419922	[redacted]	[redacted]	TLSv1	197	Ignored Unknown Record
144	7.420898	[redacted]	[redacted]	TCP	78	[TCP Dup ACK 140#2] sdt-lmd > pop3s [ACK] Seq=818 Ack=67850 Win=131072 Len=0 TSval=102630 TSecr=1029778839
145	7.426758	[redacted]	[redacted]	TLSv1	1414	[TCP Fast Retransmission] Application Data
146	7.426758	[redacted]	[redacted]	TCP	66	sdt-lmd > pop3s [ACK] Seq=818 Ack=69381 Win=131072 Len=0 TSval=102630 TSecr=1029778839
147	7.438476	[redacted]	[redacted]	TLSv1	99	Application Data
148	7.584961	[redacted]	[redacted]	TCP	66	pop3s > sdt-lmd [ACK] Seq=69381 Ack=851 Win=7872 Len=0 TSval=1029779033 TSecr=102630
149	7.757812	[redacted]	[redacted]	TCP	1414	[TCP segment of a reassembled PDU]

Figura 56: Problemas encontrados durante la sesión POP3

Seguidamente mostraremos los errores señalados en la traza correspondiente:

i. Previous segment lost



```
⊟ Transmission Control Protocol, Src Port: pop3s (995), Dst Port: sdt-lmd (3319), Seq: 65000, Ack: 818, Len: 154
    Source port: pop3s (995)
    Destination port: sdt-lmd (3319)
    [Stream index: 3]
    Sequence number: 65000    (relative sequence number)
    [Next sequence number: 65154    (relative sequence number)]
    Acknowledgement number: 818    (relative ack number)
    Header length: 32 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 123
    [Calculated window size: 7872]
    [Window size scaling factor: 64]
  ⊞ Checksum: 0x0c3e [validation disabled]
  ⊞ Options: (12 bytes)
  ⊟ [SEQ/ACK analysis]
    ⊟ [TCP Analysis Flags]
      ⊟ [A segment before this frame was lost]
        ⊟ [Expert Info (Warn/Sequence): Previous segment lost (common at capture start)]
            [Message: Previous segment lost (common at capture start)]
            [Severity level: Warn]
            [Group: Sequence]
    TCP segment data (154 bytes)
```

Figura 57: Detalles trama Previous Segment Lost

Este tipo de error nos muestra que durante la transferencia de datos entre el cliente y el servidor de correo, se ha perdido el paquete de ese segmento esperado.

ii. Duplicated ACK

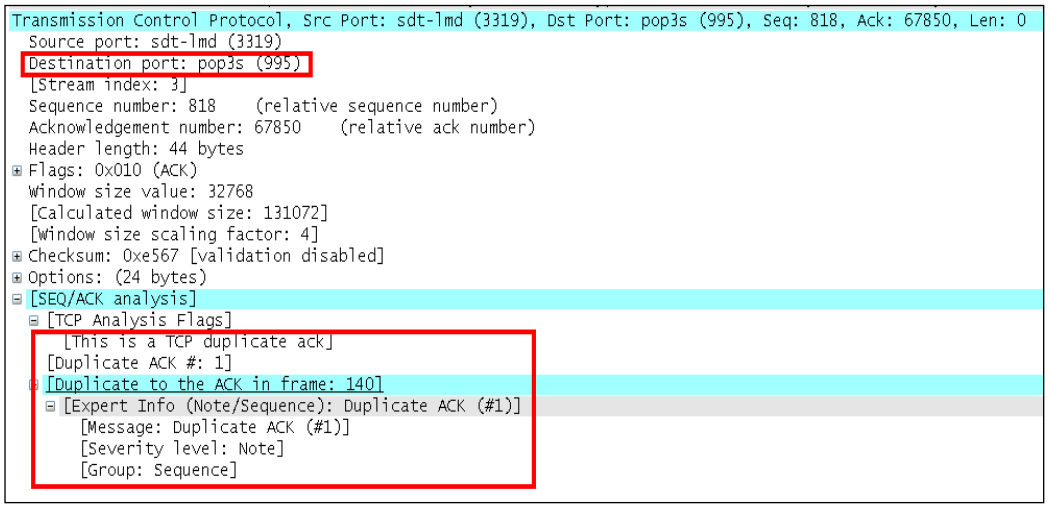


Figura 58: Detalles trama Duplicated Ack

El hecho de que sea necesario retransmitir de nuevo una trama determinada, vemos como se envía este mensaje de control, de confirmación de la otra trama retransmitida. El cliente envía un paquete TCP Dup ACK al servidor, solicitando enviar el paquete perdido. Así, el cliente seguirá enviando ACKs duplicados hasta que atiendan la petición requerida. Estos ACKs pueden ser problemas de la red implementada, porque pueden deberse a retardo por una congestión de la misma.

iii. Fast Retransmission

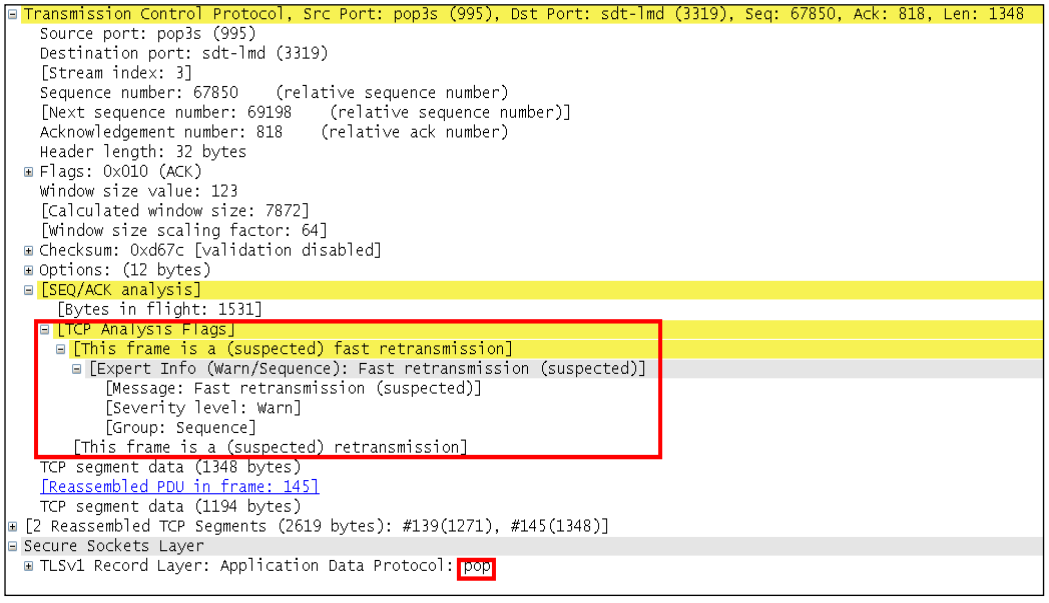


Figura 59: Detalles trama Fast Retransmission

Este mecanismo aparece cuando se reciben 3 ACKs duplicados, y consiste en una retransmisión d segmento perdido.

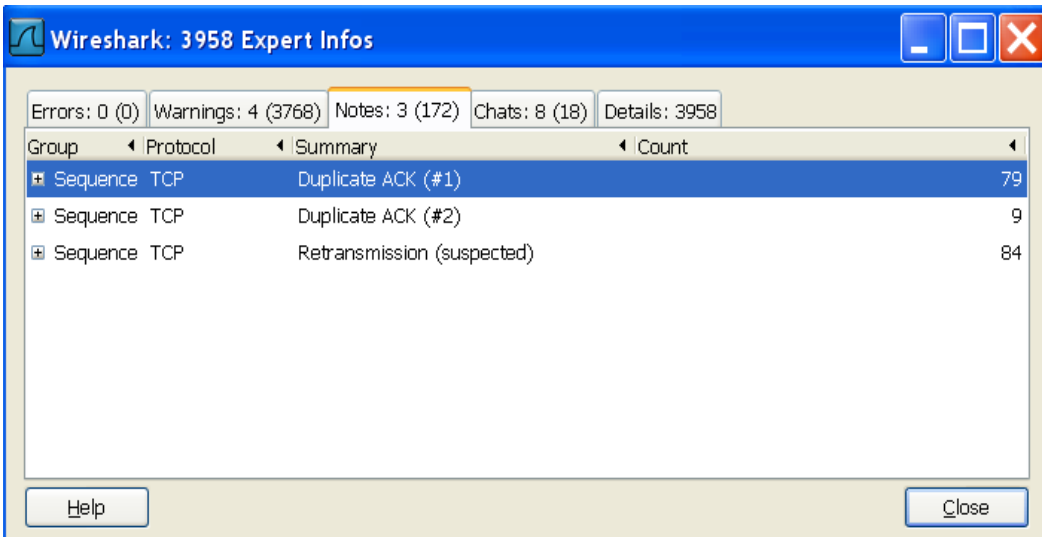


Figura 60: Detalles mecanismo Fast Retransmission

Vemos como se esperan retransmisiones con 3 ACKs duplicados, incluido en el mensaje *Retransmission suspected.*

En este caso, el comportamiento del tráfico de la aplicación POP3 se representa de esta forma:

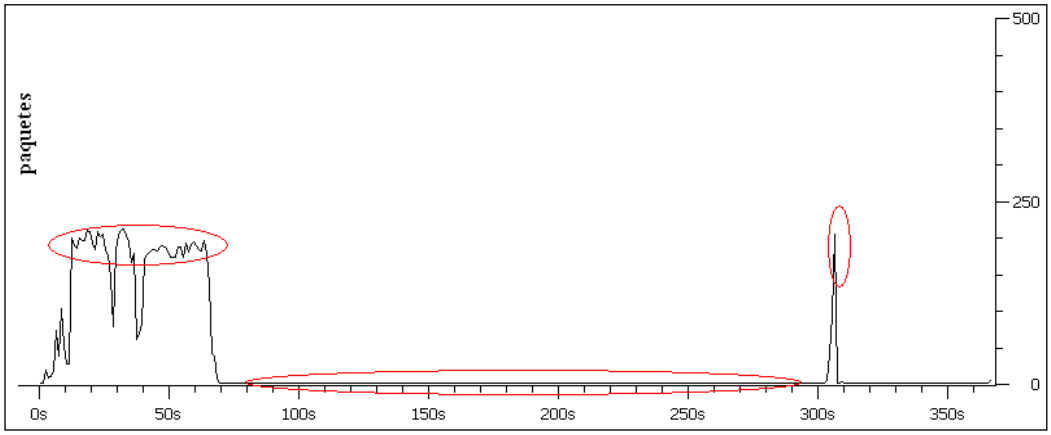


Figura 61: Evolución tráfico durante la sesión POP3 establecida

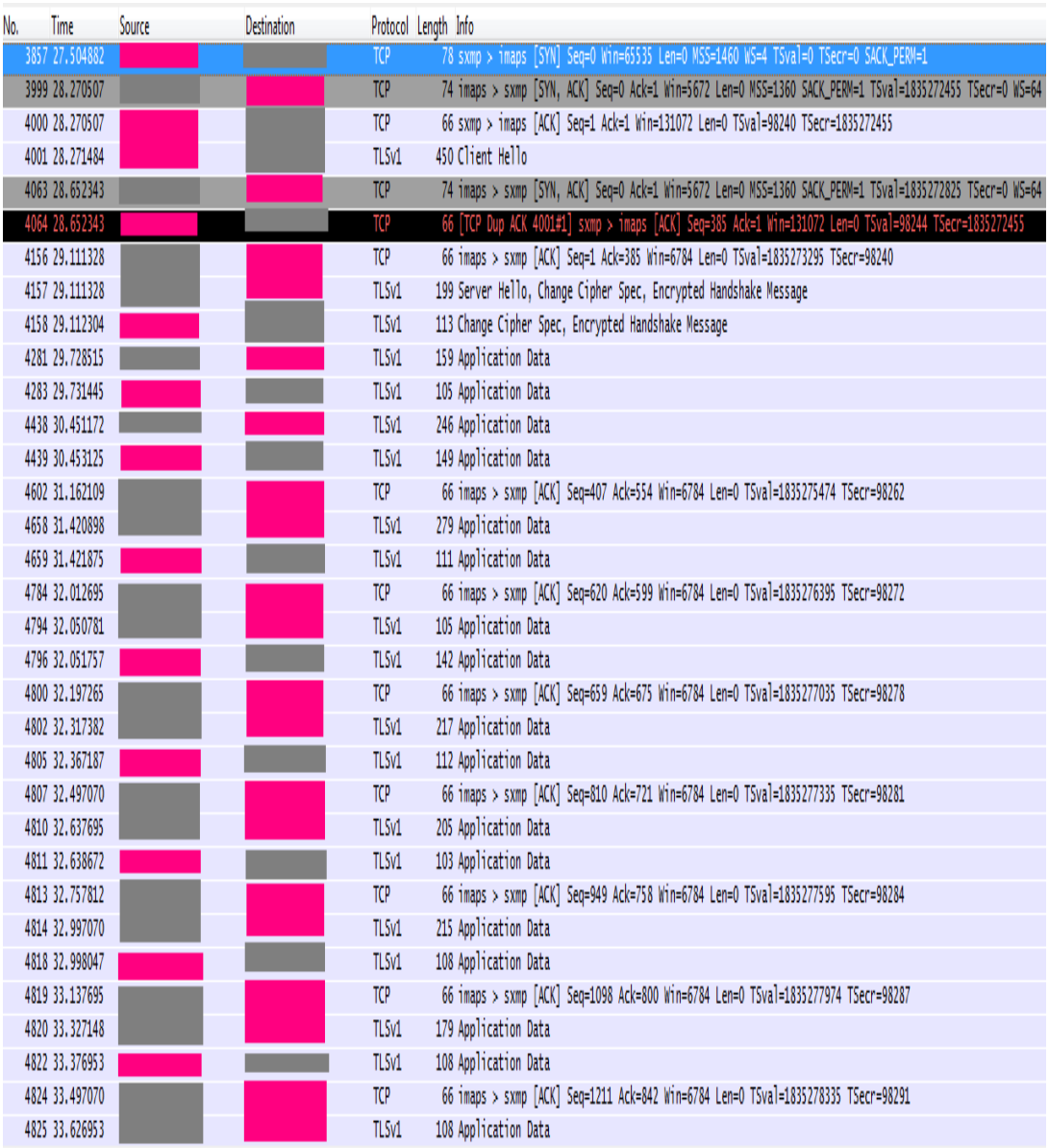
Al igual que ocurre con las aplicaciones que intercambian información entre cliente y servidor, el comportamiento del trafico mantiene generalmente la forma que aparece en estas graficas: zonas de valles donde no existe intercambio de paquetes, es decir, de volumen que se puede contabilizar. Por otro lado aparecen zonas donde se envía la información requerida por el cliente, aunque ese envío no es espaciado en el tiempo, más bien aparece en determinados momentos, que se repiten con cierta periodicidad.

3.3.3.2.2. IMAP

En este caso, mostramos como acceder a una cuenta de correo electrónico a través del protocolo IMAP, que a diferencia del protocolo anterior obtendrían tiempo de respuesta más rápidos ya que mantienen la interfaz establecida durante todo momento.

Puesto que las trazas relacionadas con el protocolo TLSv1 las estudiaremos posteriormente, en este apartado comprobaremos únicamente las comprometidas con el protocolo IMAP.

Si nos fijamos en la información de la traza correspondiente al protocolo sobre el que se establece el protocolo de red IMAP, obtenemos la siguiente información:



No.	Time	Source	Destination	Protocol	Length	Info
3857	27.504882			TCP		78 sxmp > imaps [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 TSval=0 TSecr=0 SACK_PERM=1
3999	28.270507			TCP		74 imaps > sxmp [SYN, ACK] Seq=0 Ack=1 Win=5672 Len=0 MSS=1360 SACK_PERM=1 TSval=1835272455 TSecr=0 WS=64
4000	28.270507			TCP		66 sxmp > imaps [ACK] Seq=1 Ack=1 Win=131072 Len=0 TSval=98240 TSecr=1835272455
4001	28.271484			TLSv1		450 Client Hello
4063	28.652343			TCP		74 imaps > sxmp [SYN, ACK] Seq=0 Ack=1 Win=5672 Len=0 MSS=1360 SACK_PERM=1 TSval=1835272825 TSecr=0 WS=64
4064	28.652343			TCP		66 [TCP Dup ACK 4001#1] sxmp > imaps [ACK] Seq=385 Ack=1 Win=131072 Len=0 TSval=98244 TSecr=1835272455
4156	29.111328			TCP		66 imaps > sxmp [ACK] Seq=1 Ack=385 Win=6784 Len=0 TSval=1835273295 TSecr=98240
4157	29.111328			TLSv1		199 Server Hello, Change Cipher Spec, Encrypted Handshake Message
4158	29.112304			TLSv1		113 Change Cipher Spec, Encrypted Handshake Message
4281	29.728515			TLSv1		159 Application Data
4283	29.731445			TLSv1		105 Application Data
4438	30.451172			TLSv1		246 Application Data
4439	30.453125			TLSv1		149 Application Data
4602	31.162109			TCP		66 imaps > sxmp [ACK] Seq=407 Ack=554 Win=6784 Len=0 TSval=1835275474 TSecr=98262
4658	31.420898			TLSv1		279 Application Data
4659	31.421875			TLSv1		111 Application Data
4784	32.012695			TCP		66 imaps > sxmp [ACK] Seq=620 Ack=599 Win=6784 Len=0 TSval=1835276395 TSecr=98272
4794	32.050781			TLSv1		105 Application Data
4796	32.051757			TLSv1		142 Application Data
4800	32.197265			TCP		66 imaps > sxmp [ACK] Seq=659 Ack=675 Win=6784 Len=0 TSval=1835277035 TSecr=98278
4802	32.317382			TLSv1		217 Application Data
4805	32.367187			TLSv1		112 Application Data
4807	32.497070			TCP		66 imaps > sxmp [ACK] Seq=810 Ack=721 Win=6784 Len=0 TSval=1835277335 TSecr=98281
4810	32.637695			TLSv1		205 Application Data
4811	32.638672			TLSv1		103 Application Data
4813	32.757812			TCP		66 imaps > sxmp [ACK] Seq=949 Ack=758 Win=6784 Len=0 TSval=1835277595 TSecr=98284
4814	32.997070			TLSv1		215 Application Data
4818	32.998047			TLSv1		108 Application Data
4819	33.137695			TCP		66 imaps > sxmp [ACK] Seq=1098 Ack=800 Win=6784 Len=0 TSval=1835277974 TSecr=98287
4820	33.327148			TLSv1		179 Application Data
4822	33.376953			TLSv1		108 Application Data
4824	33.497070			TCP		66 imaps > sxmp [ACK] Seq=1211 Ack=842 Win=6784 Len=0 TSval=1835278335 TSecr=98291
4825	33.626953			TLSv1		108 Application Data

Figura 62: Establecimiento sesión IMAP

Específicamente, estudiando la trama donde se inicia la sesión, obtenemos los siguientes valores relacionados con el protocolo correspondiente:

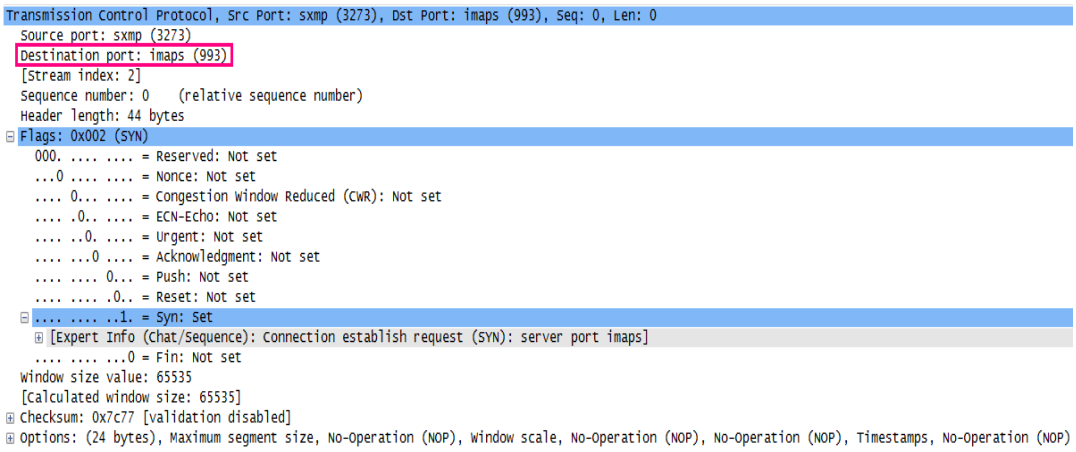


Figura 63: Detalles trama IMAP

Para evitar añadir demasiadas capturas relacionadas con las trazas que confirman cada una de las peticiones entre cliente y servidor, añadimos a continuación, el flujo de datos entre cliente y servidor de una sesión establecida correctamente.

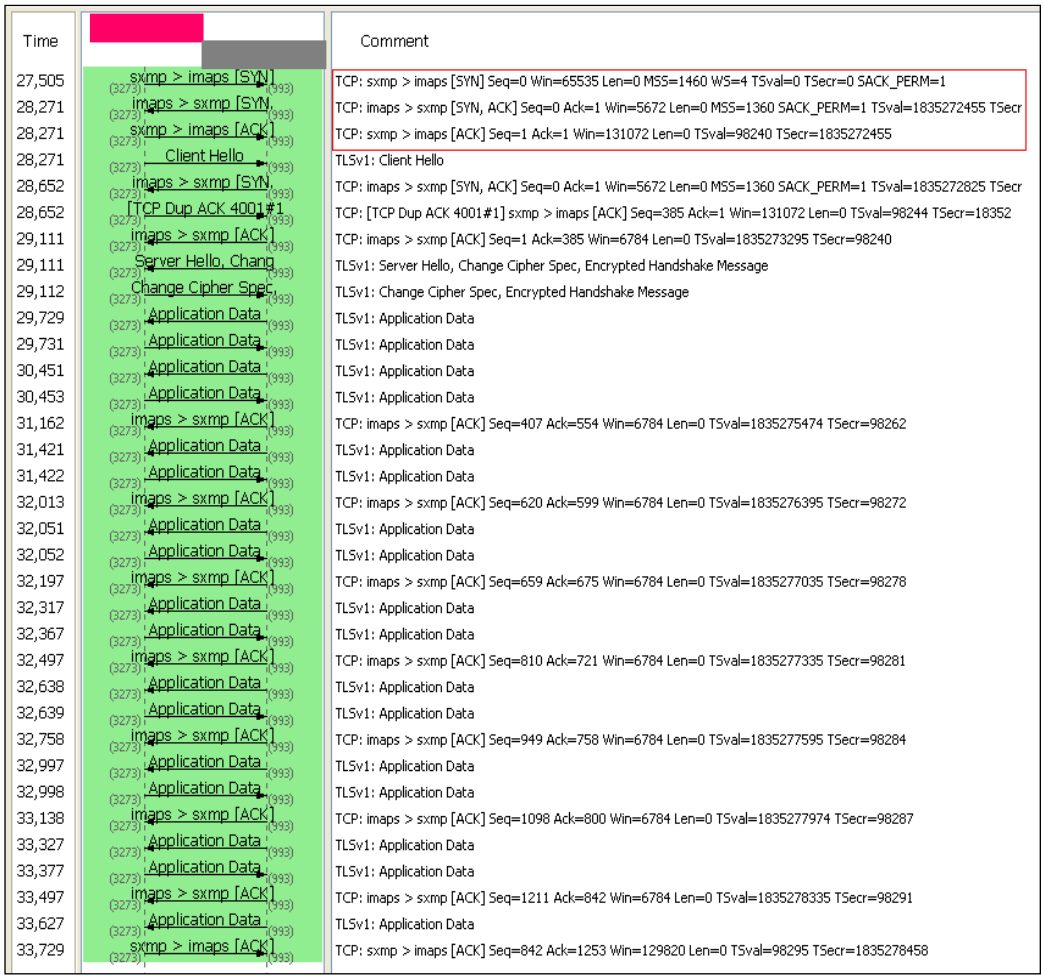


Figura 64: Flujo tramas de una sesión IMAP establecida

En este caso, la tendencia del trafico es diferente que en el caso del protocolo anterior aunque se utilicen ambos para poder acceder a los servicios de correo electrónico.

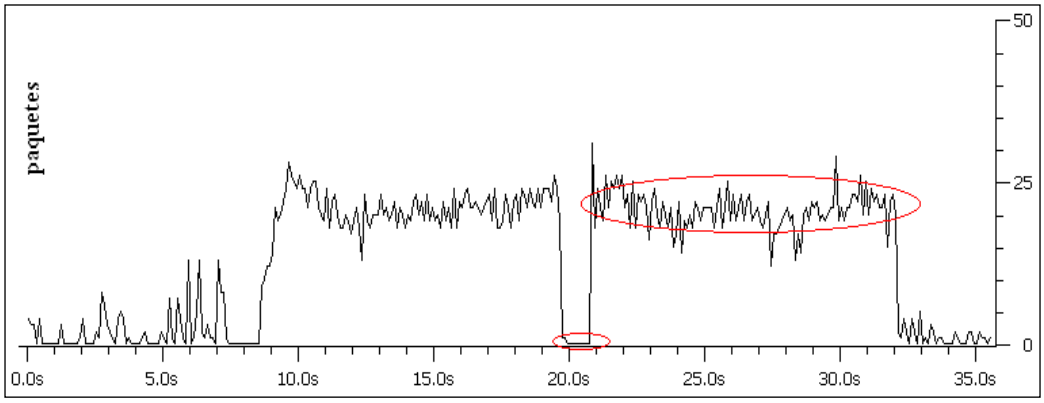


Figura 65: Evolución tráfico durante la sesión IMAP establecida

Como podemos comprobar, no existen momentos puntuales en los que exista una gran transacción de paquetes con información, si no que esos momentos están prolongados en el tiempo. La explicación es sencilla, pues el hecho de que mantengan la conexión de forma continuada entre ambos extremos, el número de paquetes que se envían aumenta en menor tiempo. Además verificamos que existen muy pocas zonas valle, en las que no se transmite demasiada información.

Al igual que en protocolos anteriores comprobamos la existencia de errores, de tipo retransmisiones, ACK duplicados, fragmentos perdidos… pero que se deben a los errores comunes en estas sesiones establecidas de forma continuada.

3.3.3.4 P2P: BitTorrent

En este caso, la aplicación P2P BitTorrent por su propia definición, mostrará cómo se van intercambiando archivos entre los nodos que forman el entramado de esta red en la que todos los nodos pueden ser cliente y servidores del archivo requerido.

Como comprobamos en el siguiente flujo de tramas, se realizan peticiones basados en el protocolo UDP, entre los distintos nodos que forman la red BitTorrent:

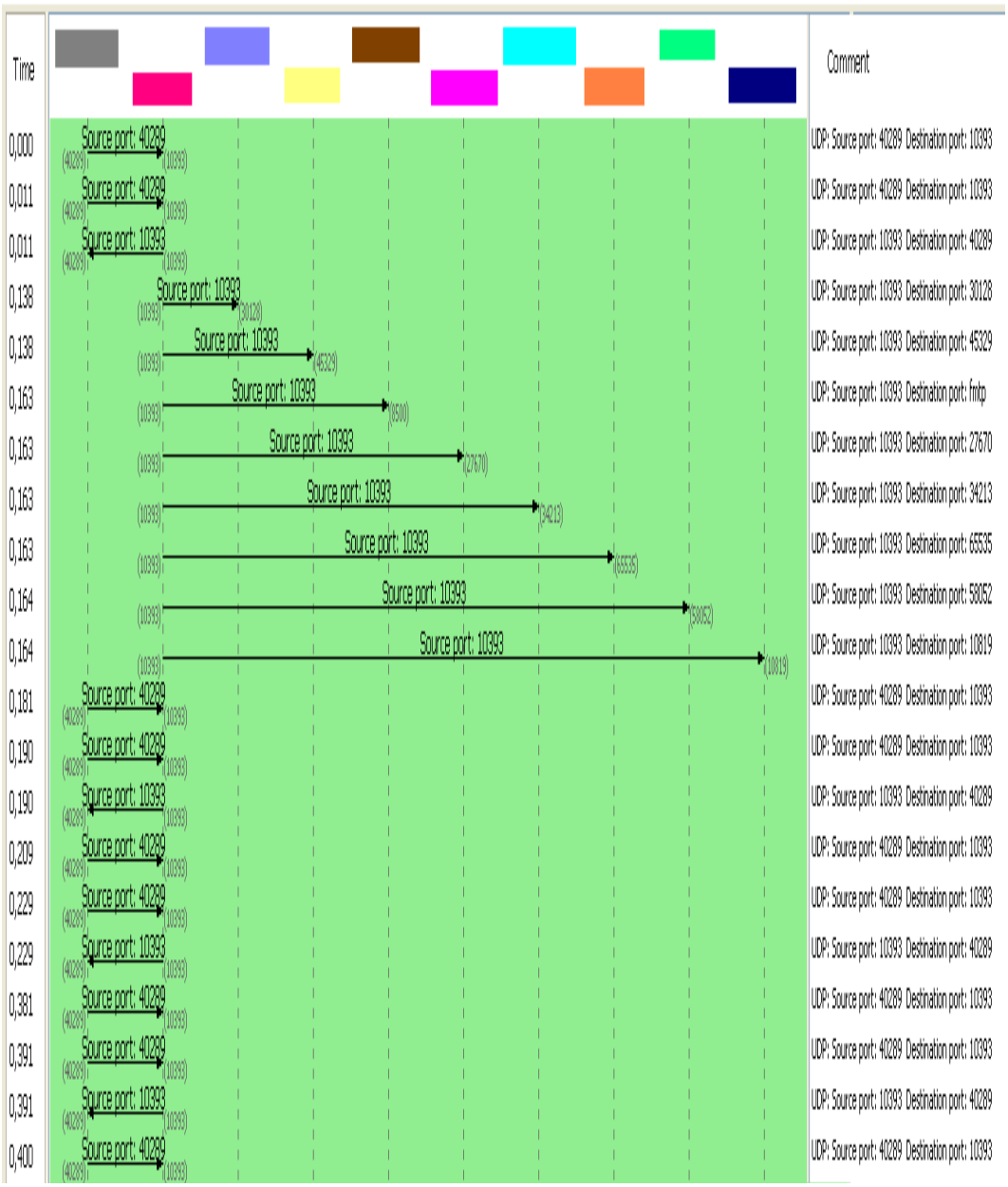


Figura 66: Flujo tramas UDP entre nodos forman red BitTorrent

Los valores que podemos comprobar en los mensajes UDP contendrían los siguientes datos:

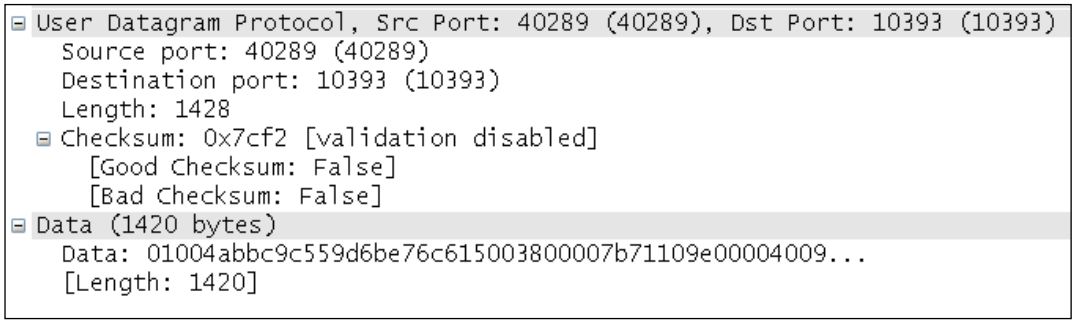


Figura 67: Detalles mensajes UDP

Hasta que se origina el archivo origen y se transmite a través de la red de servidores-clientes entre unos nodos y otros:

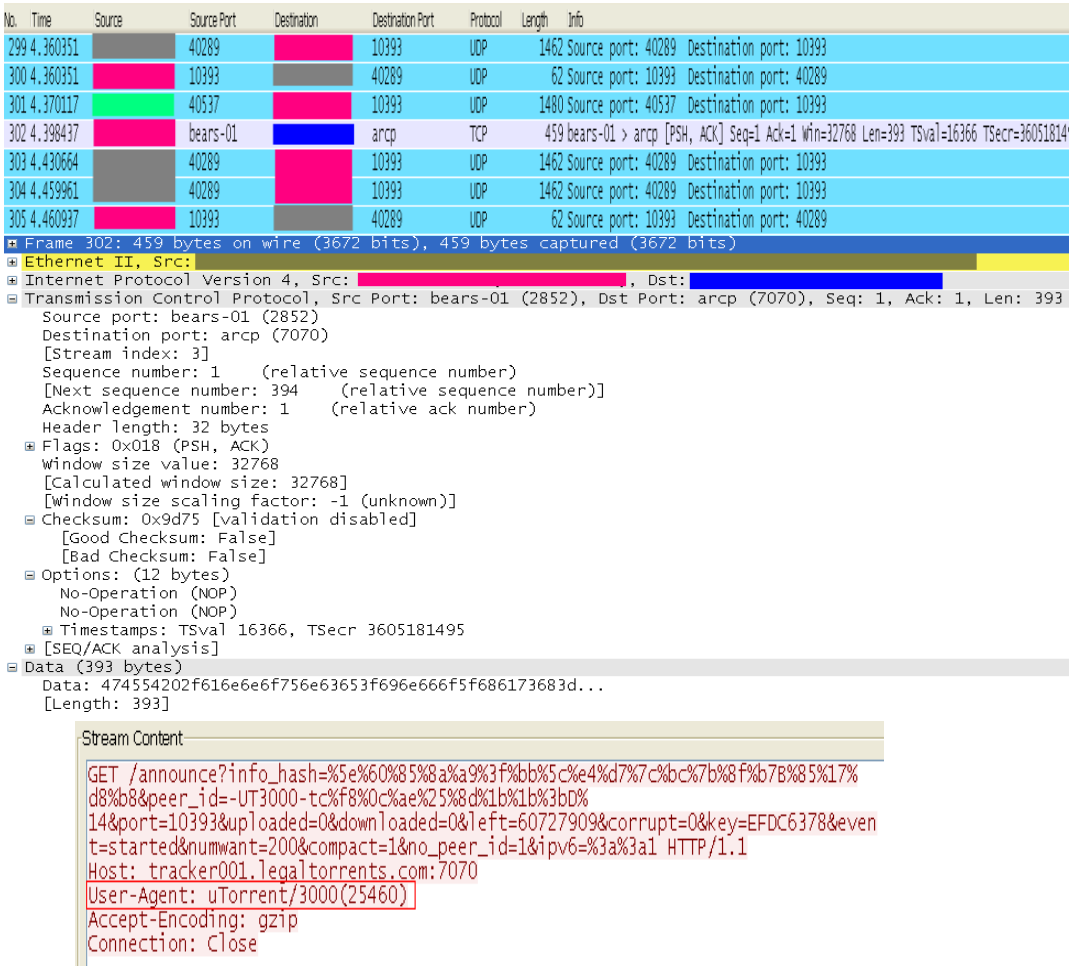


Figura 68: Intercambio archivo origen entre redes de nodos

También hemos encontrado algunos errores durante las pruebas de este protocolo:

Destination Unreachable

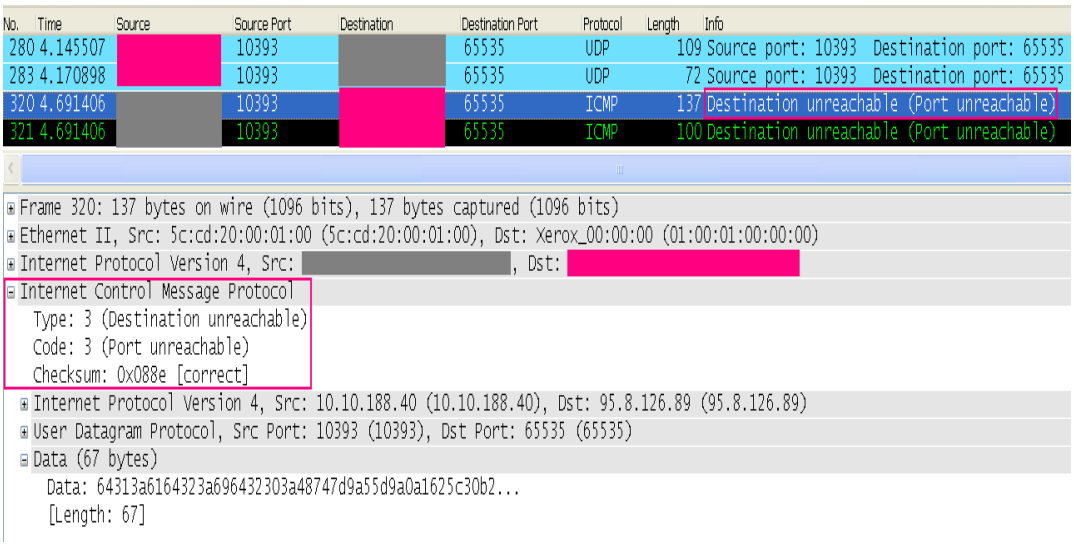


Figura 69: Detalles trama Destination Unreachable

Este error consiste tal y como indica el código de error, que el protocolo de UDP es incapaz de demultiplexar el datagrama en la capa de transporte del destino final, y por lo tanto no existe mecanismo para informar al que le envió el paquete.

La tendencia en este tipo de aplicaciones resultó ser la esperada, gran envío de paquetes de información durante todo el tiempo en el que se ha mantenido la captura de la sesión establecida:

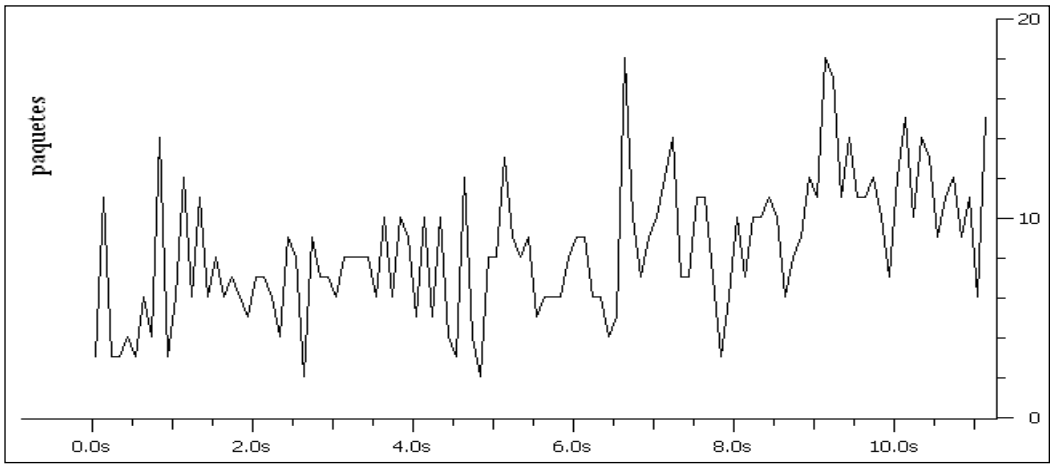


Figura 70: Evolución tráfico durante la sesión de la aplicación P2P establecida

3.3.3.5 Youtube

Mostraremos como son las trazas capturadas desde que nos dirigimos a la página de *Youtube* hasta que accedo al vídeo que deseo visualizar, y así recoger la información suficiente para analizar las capturas del tráfico, siendo la mayor parte de tipo HTTP y TCP cuyos métodos analizaremos.

La traza completa la mostramos a continuación, para ir después mostrando los valores de cada una de las tramas enviadas.

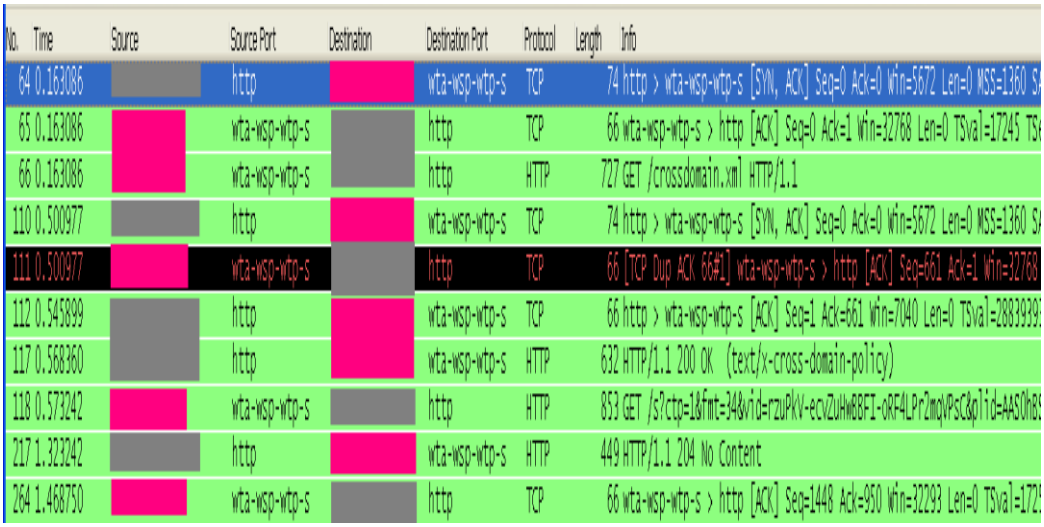


Figura 71: Flujo tramas durante el establecimiento sesión *Youtube*

El flujo completo que obtenemos es el siguiente:

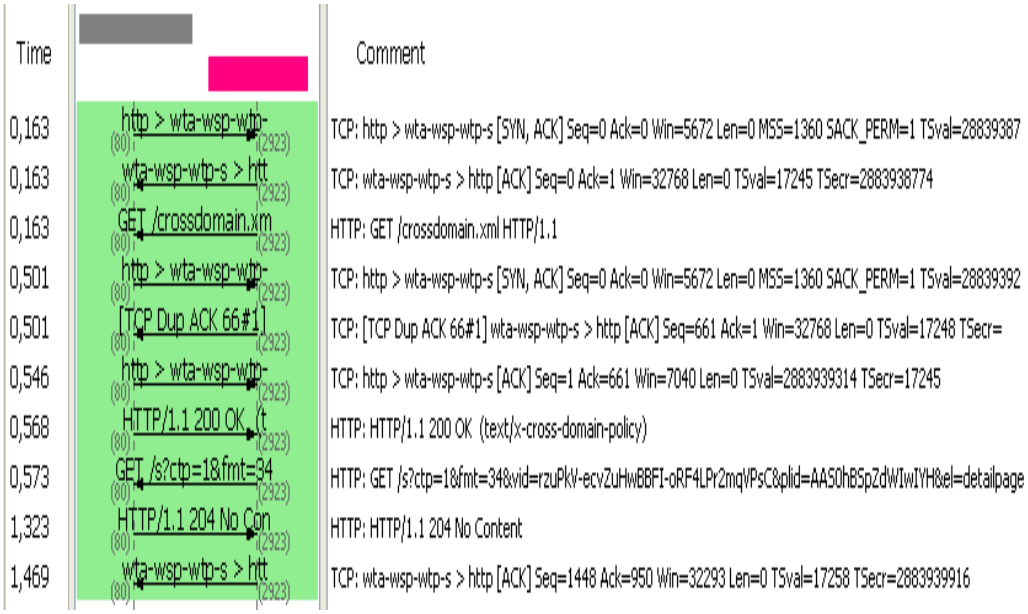


Figura 72: Establecimiento sesión *Youtube* establecida

Para poder comprender los valores de las trazas de una forma más completa, presentamos el flujo de los datos de este modo, señalando las peticiones donde comprobamos que visualizamos el vídeo requerido.

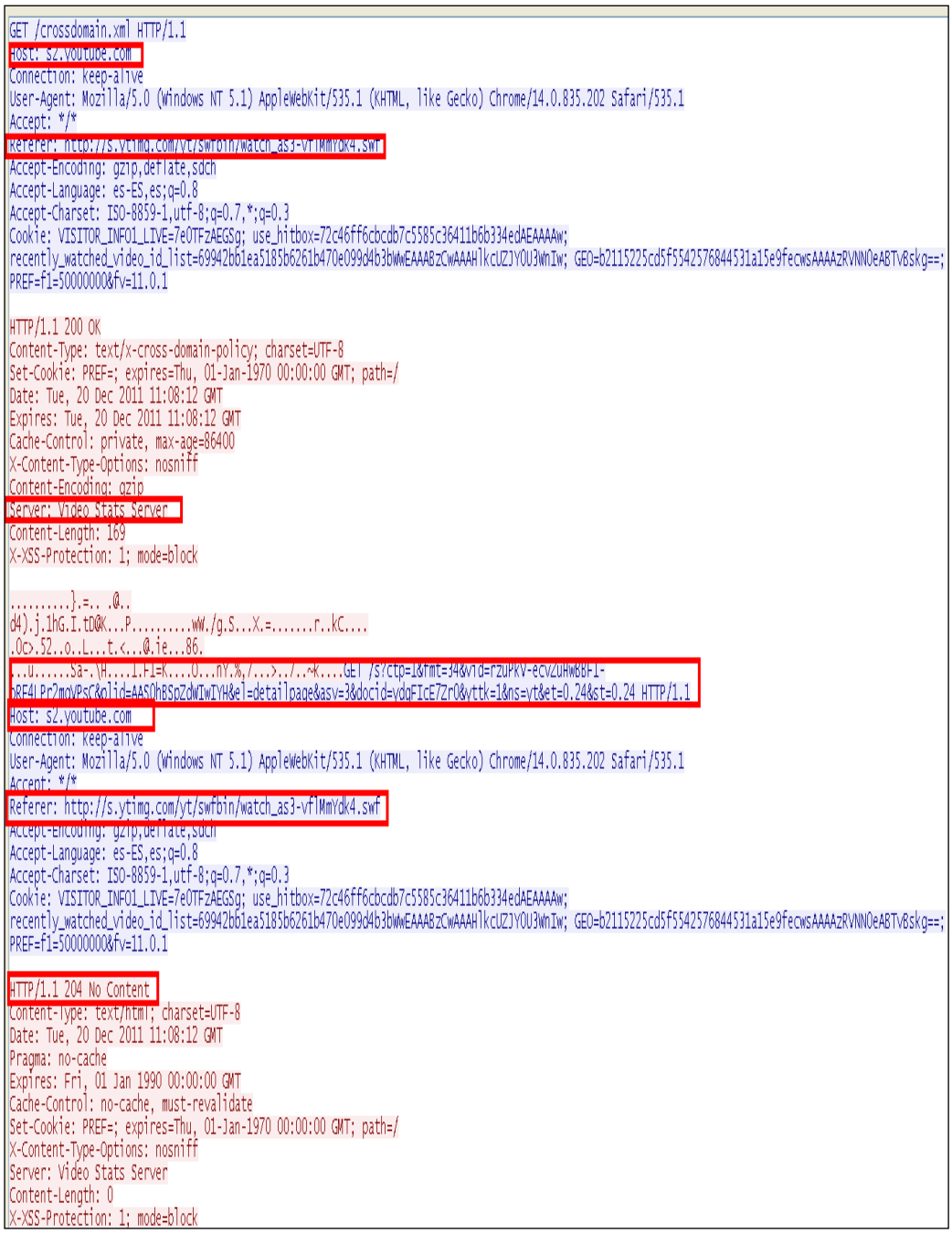


Figura 73: Detalles trama sesión acceso al vídeo de Youtube

Los valores codificados para los resultados de los métodos HTTP significarían lo siguiente:

HTTP/1.1 200 OK: Se ha descargado con éxito, la petición iniciada.
HTTP/1.1 204 No Content: La información no es el conjunto definitiva disponible en el servidor del origen.

De nuevo aparece en esta sesión, un error relacionado con las retransmisiones de tipo TCP, que como hemos explicado anteriormente es debido a problemas de congestión de la red.

El comportamiento de las aplicaciones de *streaming,* en este caso empleando *youtube* como ejemplo, resulta ser de la siguiente forma:

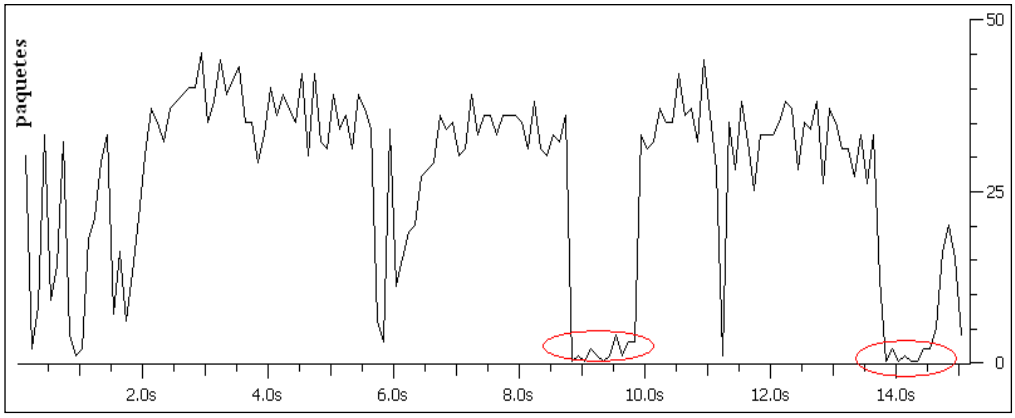


Figura 74: Evolución tráfico durante la sesión Youtube establecida

Podemos comprobar cómo al principio existen picos en los que existe envío de paquetes, previos a que comience el vídeo que deseamos ver. Sin embargo, una vez se inicia la visualización, vemos como el aspecto del tráfico muestra un patrón que se mantiene durante los mismos instantes de tiempo.

Claramente se reflejan los valores pico como los periodos en los que se visualizan las imágenes, y los valores valle donde se almacena el tráfico que se visualizará posteriormente.

3.3.3.6 Skype

En este apartado veremos el comportamiento de la aplicación de *Skype*, a pesar de que es bastante complicado descifrarlo completamente ya que emplea mecanismos de cifrado potentes, pues debe controlar el uso de VoIP gracias a la tecnología P2P.

Veremos que se emplea bastante el uso del protocolo UDP para las conexiones con varios servicios ya que no afecta significativamente a la congestión de Internet.

Es lógico que se emplee para este tipo de aplicaciones de streaming y vídeo pues por su propia naturaleza, este protocolo depende de la aplicación que recibe el mensaje para procesar y comprobar la entrega correcta, aunque se vayan enviando paquetes mientras tanto.

Dado que existe mucha información para poder resumirla en este punto, mostraremos el intercambio de trazas existente entre los puertos que ofrecen los servicios más comunes que suelen aparecer en esta aplicación. Aunque es cierto que muchos de los servicios están cifrados y no podemos concluir exactamente a cuál corresponden:

Puerto **40001:** Esta conexión es necesaria para que se oiga la voz en la conferencia existente. Importante habilitar este puerto en el lado del usuario.

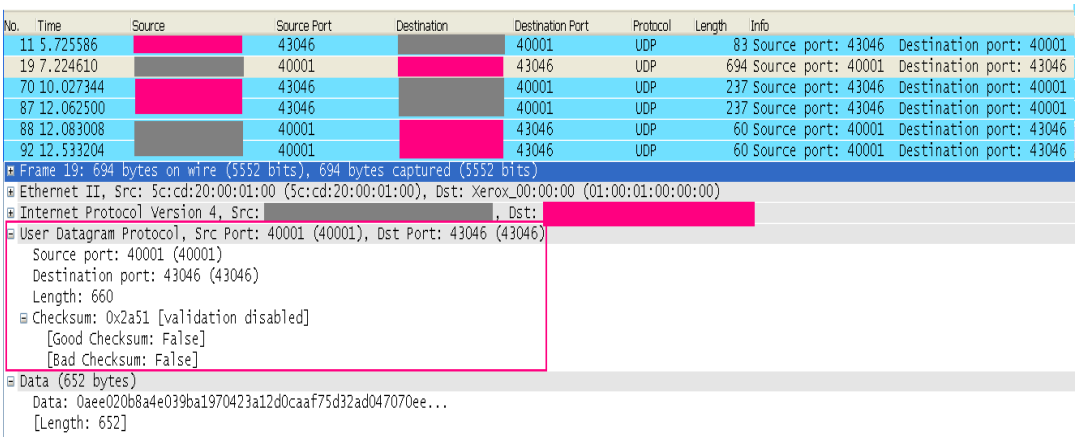


Figura 75: Detalle trama puerto 40001

Puerto **12350:** Puerto donde se establece la conexión.

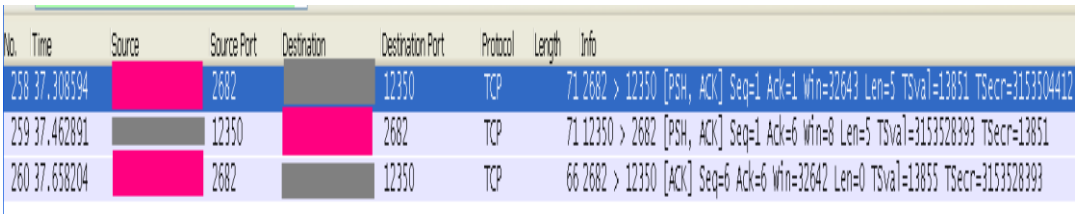


Figura 76: Detalle trama puerto 12350

Aparecen otros puertos como:

- Tqdata-27000
- Ncdmirroring-2706
- Vspread-2695
- https-443
- rsp-2682
- belarc-http-2693
- Algunos otros que están registrados y cuyo servicio no podemos conocer

Como en anteriores pruebas, hemos comprobado que aparecen errores de tipo TCP, donde se especifica la necesidad de retransmisiones de trazas. Correspondería con los mismos problemas existentes y definidos en la red.

Finalmente añadimos un extracto del establecimiento de una conexión *Skype*

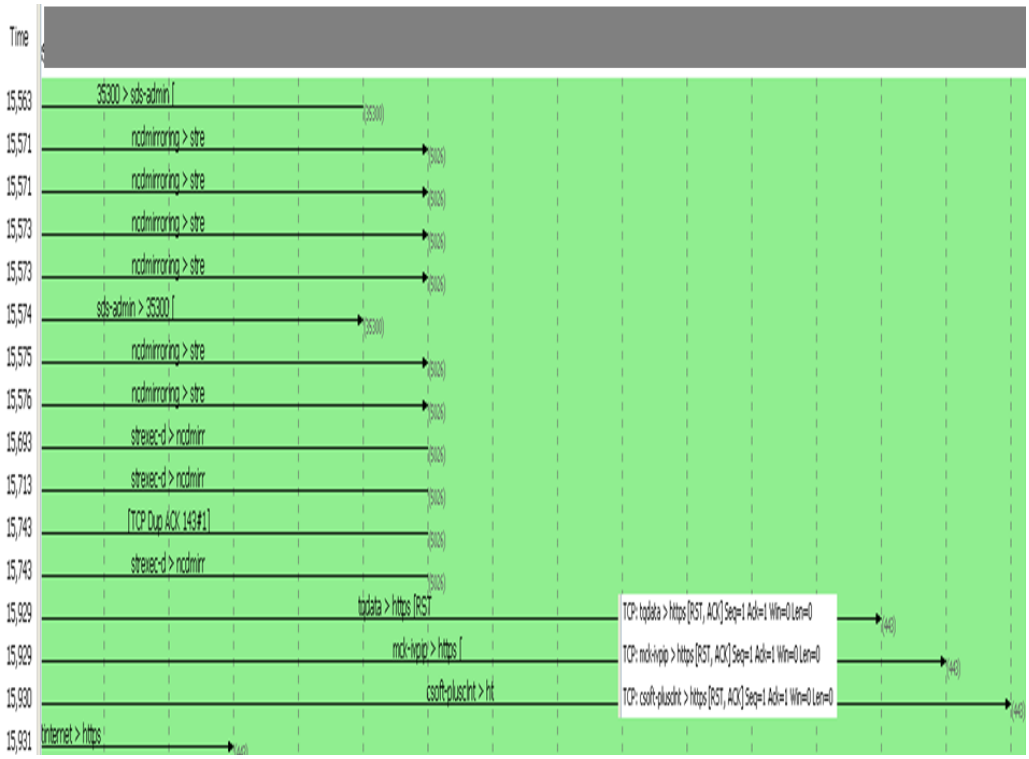


Figura 77: Flujo establecimiento sesión *Skype*

El comportamiento del tráfico extraído en la sesión del protocolo de *Skype* presenta la siguiente apariencia:

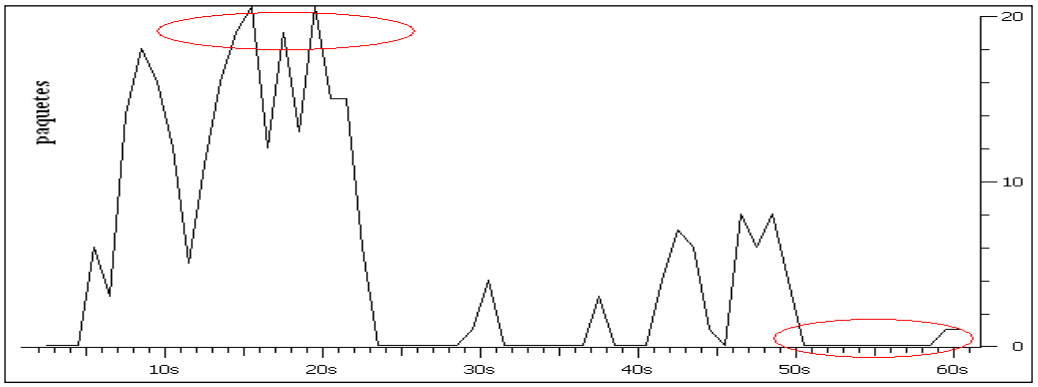


Figura 78: Evolución tráfico durante la sesión *Skype* establecida

Con esta gráfica es complicado obtener unas conclusiones en las que poder obtener explicaciones contundentes. Podríamos pensar que la información relativa al inicio de sesión, el inicio de la conexión con los servicios necesarios y otras conexiones cerradas, se realiza al principio de la conexión. Mientras que al final de la captura, aparecen valles que muestran que ya está establecida la conexión entre los dos nodos y que no intercambian paquetes con grandes informaciones.

3.3.3.7 IPSec

En este apartado comprobamos que puede establecerse un túnel IPSec a través del equipo NATBOX, que realiza las traducciones de direcciones.

Comprobamos que se establece el túnel a través del protocolo UDP y mostramos los puertos configurados para el establecimiento.

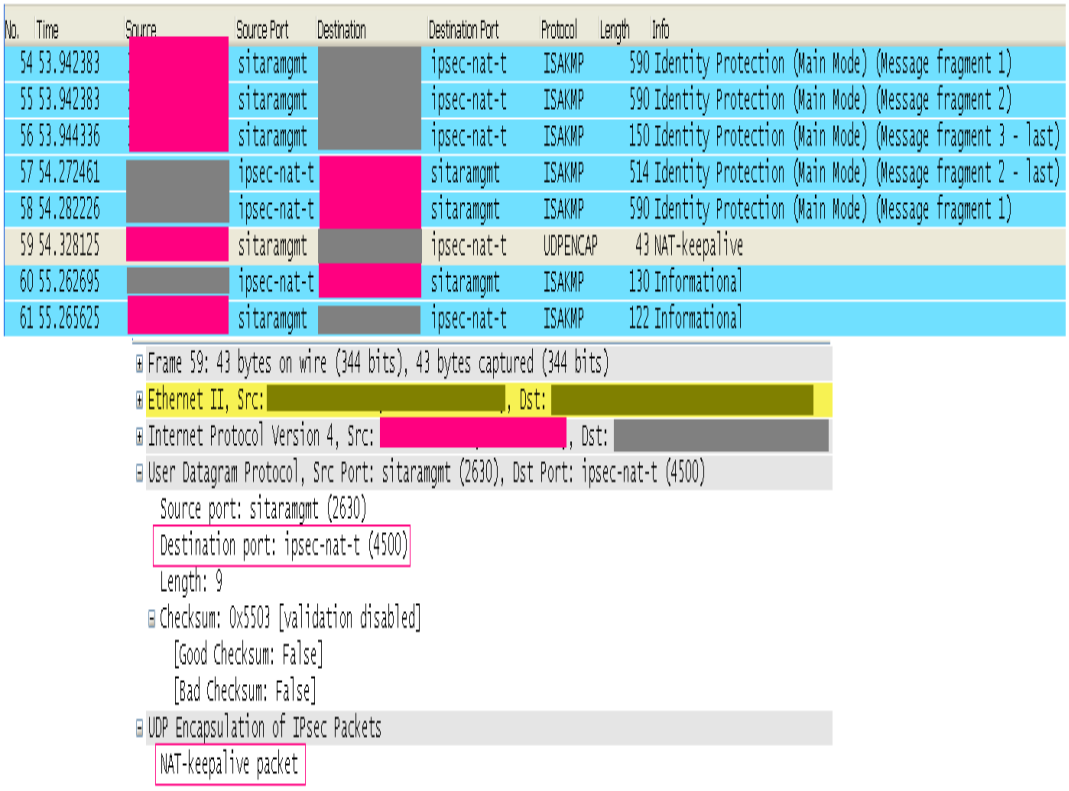


Figura 79: Establecimiento túnel IPSec

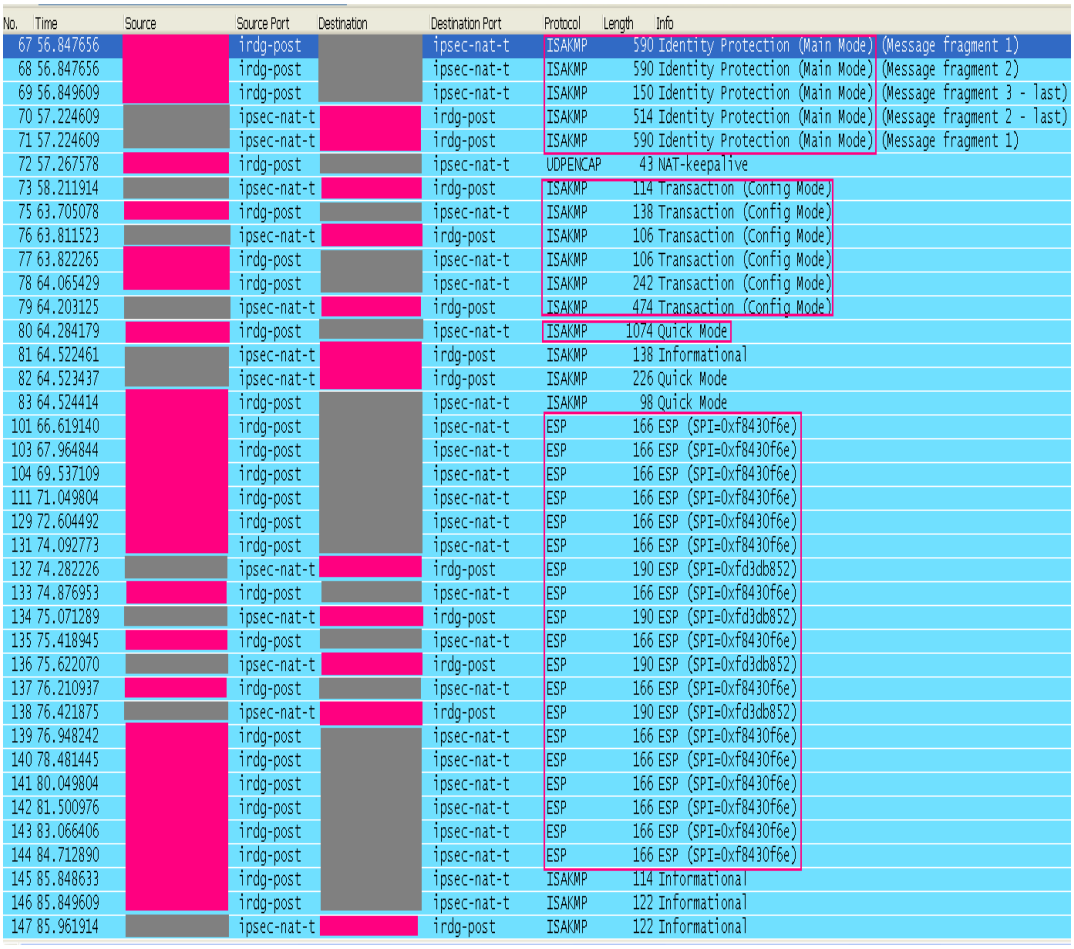
A continuación mostraremos como se establecen los cifrados del túnel establecido. A través del protocolo ISAKMP que contiene toda la información requerida para la ejecución del servicio que estamos observando [26].

Se emplea como marco común para acordar la negociación de las claves, ya que es independiente de la técnica de generación de clave.

En la fase 1, vemos como el equipo **NATBOX** establece un canal seguro con el punto de acceso a Internet con el que comunicarse. Tal y como aparece en la siguiente captura como *Main Mode*.

En la siguiente fase 2, se negocian las asociaciones de seguridad en nombre del servicio que necesite claves y/o parámetros. El nombre de esta fase es lo que se conoce como *Quick Mode.*

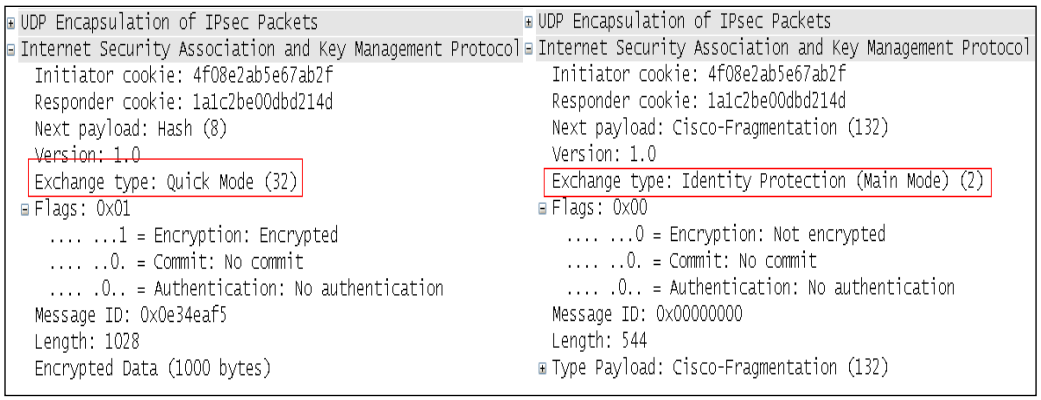
Veremos también que el protocolo ESP se emplea para ofrecer mayor confidencialidad y autenticación en el origen de datos.



No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
67	56.847656		irdg-post		ipsec-nat-t	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 1)
68	56.847656		irdg-post		ipsec-nat-t	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 2)
69	56.849609		irdg-post		ipsec-nat-t	ISAKMP	150	Identity Protection (Main Mode) (Message fragment 3 - last)
70	57.224609		ipsec-nat-t		irdg-post	ISAKMP	514	Identity Protection (Main Mode) (Message fragment 2 - last)
71	57.224609		ipsec-nat-t		irdg-post	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 1)
72	57.267578		irdg-post		ipsec-nat-t	UDPENCAP	43	NAT-keepalive
73	58.211914		ipsec-nat-t		irdg-post	ISAKMP	114	Transaction (Config Mode)
75	63.705078		irdg-post		ipsec-nat-t	ISAKMP	138	Transaction (Config Mode)
76	63.811523		ipsec-nat-t		irdg-post	ISAKMP	106	Transaction (Config Mode)
77	63.822265		irdg-post		ipsec-nat-t	ISAKMP	106	Transaction (Config Mode)
78	64.065429		irdg-post		ipsec-nat-t	ISAKMP	242	Transaction (Config Mode)
79	64.203125		ipsec-nat-t		irdg-post	ISAKMP	474	Transaction (Config Mode)
80	64.284179		irdg-post		ipsec-nat-t	ISAKMP	1074	Quick Mode
81	64.522461		ipsec-nat-t		irdg-post	ISAKMP	138	Informational
82	64.523437		ipsec-nat-t		irdg-post	ISAKMP	226	Quick Mode
83	64.524414		irdg-post		ipsec-nat-t	ISAKMP	98	Quick Mode
101	66.619140		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
103	67.964844		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
104	69.537109		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
111	71.049804		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
129	72.604492		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
131	74.092773		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
132	74.282226		ipsec-nat-t		irdg-post	ESP	190	ESP (SPI=0xfd3db852)
133	74.876953		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
134	75.071289		ipsec-nat-t		irdg-post	ESP	190	ESP (SPI=0xfd3db852)
135	75.418945		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
136	75.622070		ipsec-nat-t		irdg-post	ESP	190	ESP (SPI=0xfd3db852)
137	76.210937		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
138	76.421875		ipsec-nat-t		irdg-post	ESP	190	ESP (SPI=0xfd3db852)
139	76.948242		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
140	78.481445		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
141	80.049804		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
142	81.500976		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
143	83.066406		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
144	84.712890		irdg-post		ipsec-nat-t	ESP	166	ESP (SPI=0xf8430f6e)
145	85.848633		irdg-post		ipsec-nat-t	ISAKMP	114	Informational
146	85.849609		irdg-post		ipsec-nat-t	ISAKMP	122	Informational
147	85.961914		ipsec-nat-t		irdg-post	ISAKMP	122	Informational

Figura 80: Trazas que reflejan la autenticación de datos

Estas son las trazas relacionadas con las fases que se aplican en el protocolo ISAKMP



```
⊞ UDP Encapsulation of IPsec Packets
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 4f08e2ab5e67ab2f
    Responder cookie: 1a1c2be00dbd214d
    Next payload: Hash (8)
    Version: 1.0
    Exchange type: Quick Mode (32)
  ⊟ Flags: 0x01
      .... ...1 = Encryption: Encrypted
      .... ..0. = Commit: No commit
      .... .0.. = Authentication: No authentication
    Message ID: 0x0e34eaf5
    Length: 1028
    Encrypted Data (1000 bytes)
```

```
⊞ UDP Encapsulation of IPsec Packets
⊟ Internet Security Association and Key Management Protocol
    Initiator cookie: 4f08e2ab5e67ab2f
    Responder cookie: 1a1c2be00dbd214d
    Next payload: Cisco-Fragmentation (132)
    Version: 1.0
    Exchange type: Identity Protection (Main Mode) (2)
  ⊟ Flags: 0x00
      .... ...0 = Encryption: Not encrypted
      .... ..0. = Commit: No commit
      .... .0.. = Authentication: No authentication
    Message ID: 0x00000000
    Length: 544
  ⊞ Type Payload: Cisco-Fragmentation (132)
```

Figura 81: Detalles fases autenticación datos

Para comprobar que se ha establecido un túnel IPSec correctamente, hemos decidido aplicar una búsqueda de servicios a través del protocolo SSDP, que anuncia a través de UDP el servicio IPSEc que acaba de establecerse:

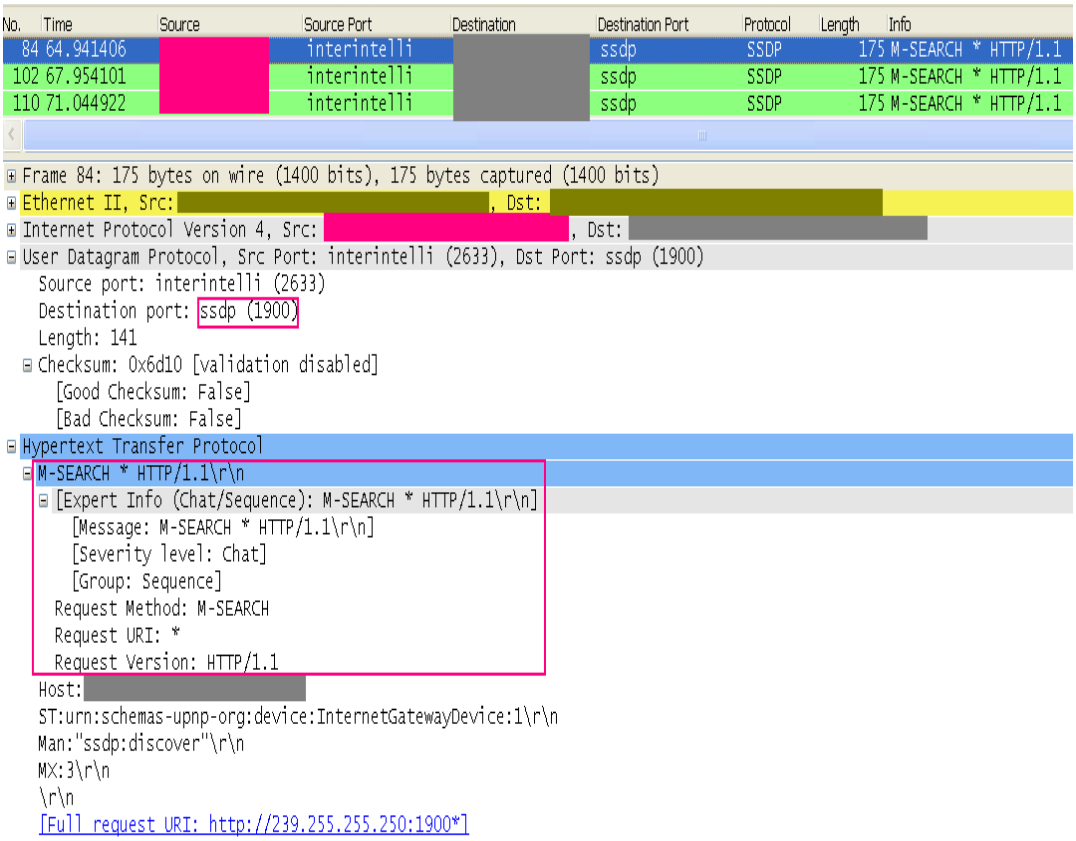


Figura 82: Detalles establecimiento túnel IPSec a través del protocolo SSDP

En este caso, comprobamos que el tráfico capturado en esta prueba tiene un comportamiento generalmente lineal. No obstante, es cierto que aparecen dos valores máximos en los que podemos concluir que son puntos clave donde existe una mayor negociación de claves y parámetros de autenticación y seguridad. Ya que durante el resto del tiempo, los valores de intercambio de información se mantienen constantes. Durante esos periodos se han realizado búsquedas de ciertos servicios UPnP, y por lo tanto también aparece cierto volumen de tráfico en esos momentos.

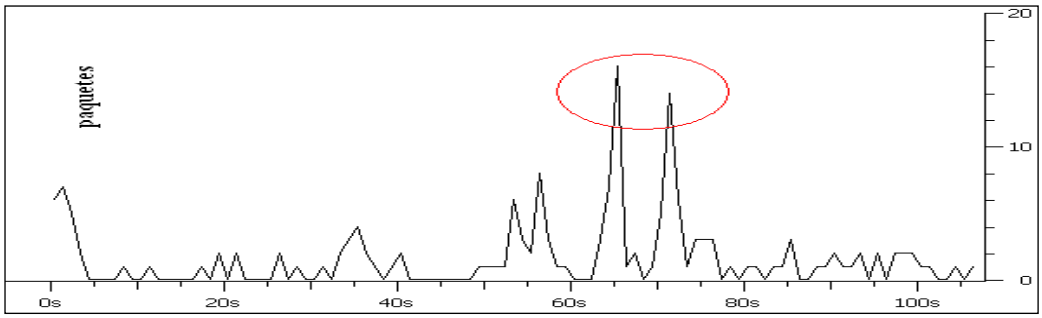


Figura 83: Evolución tráfico en el establecimiento del túnel IPSec

3.3.3.8 SSL

En este apartado comprobamos que puede establecerse correctamente una conexión SSL entre el equipo NATBOX y el acceso a Internet. Mostraremos cada una de las trazas en las que se realiza el intercambio de información para el establecimiento:

Para comprender mejor los mensajes a enviar, incluiremos un apartado donde aparecen las trazas correspondientes al establecimiento de la sesión SSL:

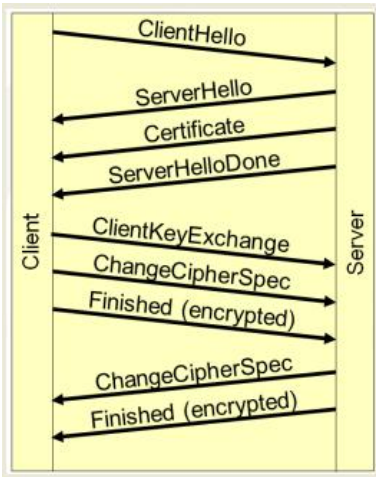


Figura 84: Funcionamiento establecimiento sesión SSL

A continuación mostraremos cada una de las trazas en donde comprobamos los mensajes entre cliente y servidor:

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
1	0.000000	[redacted]	tve-announce	[redacted]	https	TCP	78	tve-announce > https [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=4 TSval=0 TSecr=0
2	0.200196	[redacted]	https	[redacted]	tve-announce	TCP	66	https > tve-announce [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1360 SACK_PERM=1
3	0.200196	[redacted]	tve-announce	[redacted]	https	TCP	54	tve-announce > https [ACK] Seq=1 Ack=1 Win=131072 Len=0
4	0.200196	[redacted]	tve-announce	[redacted]	https	TLSv1	163	Client Hello
5	0.419922	[redacted]	https	[redacted]	tve-announce	TCP	54	https > tve-announce [ACK] Seq=1 Ack=110 Win=5888 Len=0
6	0.420899	[redacted]	https	[redacted]	tve-announce	TLSv1	140	Server Hello
7	0.548828	[redacted]	tve-announce	[redacted]	https	TCP	54	tve-announce > https [ACK] Seq=110 Ack=87 Win=130984 Len=0
8	0.729493	[redacted]	https	[redacted]	tve-announce	TLSv1	97	Change Cipher Spec, Encrypted Handshake Message
9	0.730469	[redacted]	tve-announce	[redacted]	https	TLSv1	97	Change Cipher Spec, Encrypted Handshake Message
10	0.733399	[redacted]	tve-announce	[redacted]	https	TCP	54	tve-announce > https [FIN, ACK] Seq=153 Ack=130 Win=130940 Len=0
15	0.930664	[redacted]	https	[redacted]	tve-announce	TLSv1	77	Encrypted Alert
16	0.930664	[redacted]	tve-announce	[redacted]	https	TCP	54	tve-announce > https [RST, ACK] Seq=154 Ack=153 Win=0 Len=0

Figura 85: Establecimiento sesión SSL

Cada uno de los mensajes los analizamos posteriormente:

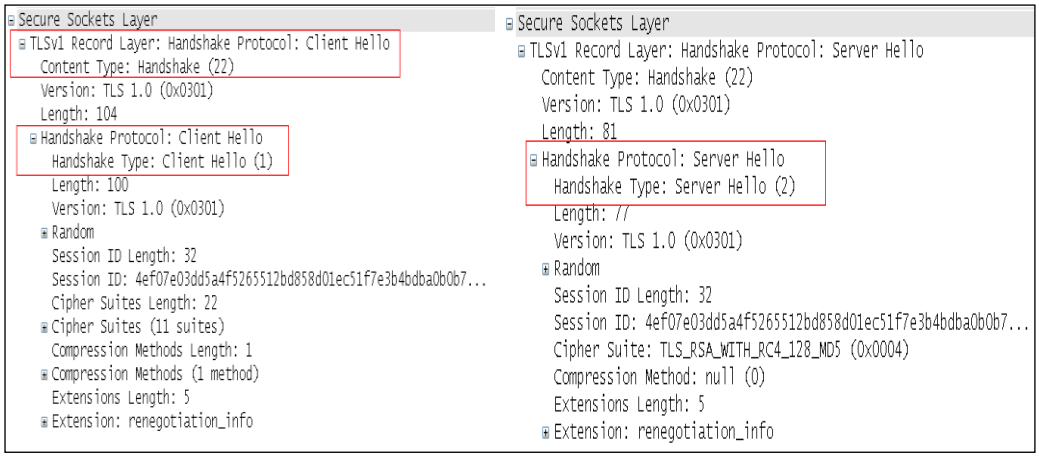


Figura 86: Detalles trazas establecimiento sesión SSL (1)

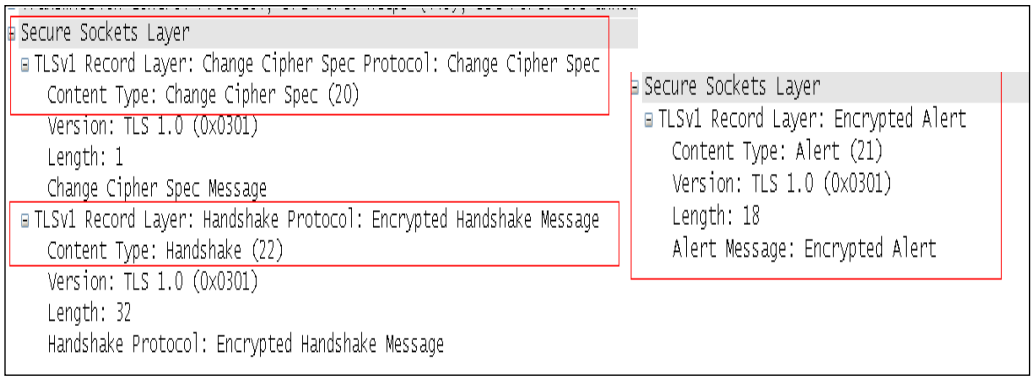


Figura 87: Detalles trazas establecimiento sesión SSL (2)

Podemos concluir que el comportamiento de este servicio basándonos en la captura de tráfico, depende de la congestión de la red. Es decir, el mayor número de paquetes se concentra durante unos momentos pero de forma desigual en la parte central de la gráfica. No existe mucha relación con la zona que ocupa, solo que durante esos momentos se han transmitido varios paquetes juntos que han sido almacenados en tiempos de menor volumen de tráfico.

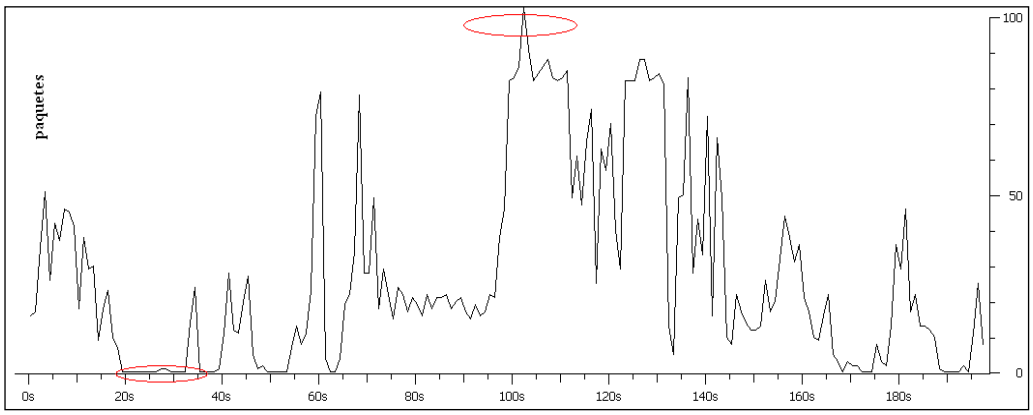


Figura 88: Evolución tráfico durante la sesión SSL establecida

4 CONCLUSIONES

Después de haber analizado el resultado de las pruebas que mostraban el comportamiento del acceso al servicio de Internet al aplicar la técnica NAT44 en una operadora móvil, hemos concluido con las siguientes valoraciones.

Las pruebas que aquí se presentan forman parte de un proceso largo de análisis por parte de varios grupos de trabajo, en los que se han decidido las soluciones para mejorar el funcionamiento y la interconexión de la red de una operadora móvil.

Es importante señalar que el número de aplicaciones a analizar tiende a infinito, por eso hemos acotado bastante el número de pruebas. Incluso en estas condiciones de contorno, el análisis es terriblemente tedioso. Muchas de las pruebas es cierto que no llevan a conclusiones claras. El hecho de que una aplicación se comporte de la forma esperada no implica que el rendimiento de la máquina que realiza las traducciones o del terminal esté empeorando, por lo tanto el número de factores a tener en cuenta para concluir de forma certera es más elevado de lo que parece.

Estos comportamientos no están reflejados estrictamente en el desarrollo de las pruebas, pero por ejemplo, cabría destacar el consumo de batería de los terminales aumentado por una incorrecta optimización de la plataforma de NATBOX.

4.1 Análisis resultados

Según los resultados obtenidos podemos confirmar ciertos comportamientos vistos en la plataforma NATBOX y señalar las conclusiones más relevantes.

- **Errores**

Permanecen abiertas multitud de conexiones TCP, ya sea por errores en las red: autenticación, direccionamiento, redirecciones, malas coberturas según la zona donde este aplicada la prueba... o incluso por ataques que se produzcan cuando por ejemplo, entramos en una red compartida tipo P2P.

Deberían valorarse formas de limitar el número de puertos que consume el usuario en el caso de la compartición de información.

Además por el hecho de compartir una dirección IP por varios usuarios, si se llega a considerar esa IP como parte de una *lista negra (spam)*, puede afectar el acceso del resto de usuarios que compartan esa IP

- **Latencias**

La mayor parte de los problemas que hemos encontrado con la plataforma de NAT son los retardos en la transmisión de paquetes debido a distintos motivos.

- Se incrementa la latencia en el punto a punto tanto de forma centralizada como distribuida, por el uso de la ruta indirecta asignada en el uso de NAT

- Debido a que algunas aplicaciones mantienen un límite de uso según la IP recibida, se retrasa la comunicación a la espera de una actualización de la base de datos de la aplicación para poder volver a acceder a ella.

- También se puede incrementar el tiempo de respuesta entre los puertos UPnP ya que los usuarios pierden el control sobre ese mapeo.

- **Temporizadores establecidos insuficientes**

El umbral establecido para borrar periódicamente las traducciones realizadas en la tabla de la plataforma NATBOX oscila los 30 minutos. Es decir, que si en ese tiempo no se ha realizado ninguna traducción, porque no se ha realizado ninguna petición de acceso al servicio, el equipo elimina los datos que contiene sus datos de traducción.

Por eso debería aumentarse la memoria RAM del equipo para poder soportar todas esas tablas de traducciones y ofrecer el servicio de los usuarios que lo requieran.

Estas pruebas que estudian la pequeña parte a la que afectan, pero si extendemos el comportamiento, esos retardos pueden verse reflejados en otros equipos que se comuniquen con el equipo GGSN al que está conectado el equipo de NAT, por eso podrían averiguarse diferentes errores que les afecten, aunque este no sea el objeto del proyecto

4.2 Trabajos futuros

En este apartado indicamos una serie de medidas posteriores que podrían desarrollarse para optimizar el acceso a Internet y sus servicios.

En trabajos futuros en los que la red de la operadora se vea expandida se puede ampliar ciertas transacciones señaladas a continuación, gracias a la escalabilidad de la plataforma NAT.

- **Redundancia Geográfica**

Sería conveniente modificar la arquitectura inicial del piloto de pruebas para evitar la congestión en zonas de máxima carga, y conseguir una redundancia geográfica. Debería incluirse un nuevo nodo que absorbiera la carga del nodo más afectado, aplicando las políticas de encaminamiento específicas para que la carga se direccione sólo en caso de incidencia.

- **Migración final IPv6**

Cuando finalmente se lleve a cabo la migración del nuevo protocolo IPv6 para ofrecer el acceso a Internet habrá que tener en cuenta ciertas consecuencias tanto en los dispositivos, acceso a las redes o sistemas punto a punto:

  - ❖ Actualizaciones y/o sustitución de ciertos equipos que deberían soportar el nuevo sistema IPv6. Aunque se podrían incorporar nuevas características del protocolo IP sin actualizar otros dispositivos de la red.

  - ❖ Es posible que ciertos fabricantes de terminales deseen modificar los accesos a la red de forma independiente.

- **Incremento Temporizadores *Timers***

Tal y como hemos comprobado en los resultados, existen muchas retransmisiones de paquetes por diversas causas, la mayor parte relacionadas con el tiempo que se mantiene establecida la sesión del usuario.

Los equipos traductores tienen configurados unos *timers* que deben ajustarse según la experiencia del usuario. Después del desarrollo de estas pruebas, sería recomendable incrementar unos minutos el temporizador del equipo NATBOX para las sesiones TCP/UDP, para que pudieran recibir todas las trazas necesarias, y que después se cerrara para minimizar el riesgo de los usuarios de recibir tráfico indeseado desde Internet.

El incremento de este temporizador sería distinto para cada clase de dispositivo, pero debe ser lo suficientemente alto para que la red o el dispositivo no reenvíen paquetes para asegurarse que la sesión continúa abierta.

En el caso de los dispositivos móviles, este incremento en el tiempo de establecimiento de sesión, reduciría el consumo de batería del terminal.

- **Independencia ALGs**

Si identificamos los *endpoints* empleando una tabla de nombre DNS, en lugar de direcciones, esto hace que las aplicaciones (ALGs) sean menos dependientes de la dirección actual que el NATBOX elige y evita el hecho de traducir el *payload* (contenido) cuando se cambia una IP.

- **Activación parámetro EIM**

Si habilitamos este parámetro tenemos una dirección IP externa estable además de un puerto (durante un periodo de tiempo determinado) que los servidores externos pueden utilizar para conectarse.

Esto significa que si proceden de un puerto de origen diferente, puede asignarse libremente una dirección externa diferente. Sería una buena solución para estabilizar las conexiones P2P.

- **Activación parámetro EIF**

Con este parámetro configurado permitimos que se conecten usuarios desde fuera a puertos que hemos abierto nosotros previamente, aunque no haya sido contra ellos.

Para conocer el detalle de en qué medida exacta se mejora el comportamiento con estos parámetros habría que ir aplicación por aplicación y hacer un análisis a bastante bajo nivel.

Para comprobar cómo funcionan las aplicaciones de forma general, lo ideal sería desactivar estos dos parámetros EIM y EIF ver si se detecta algún problema con una aplicación determinada, y luego configurarlos para esa misma en posteriores configuraciones.

5 PRESUPUESTO

En este capítulo detallamos el presupuesto desglosándolo en etapas y diferenciando el coste de cada una de las tareas. Asimismo y en función de la complejidad y los recursos utilizados durante esas tareas, se han estimado unos costes de duración basados en horas.

Inicialmente calculamos el coste relacionado con las herramientas tipo SW empleadas en el desarrollo del proyecto. Han sido necesarias estas licencias de software para poder realizar el trabajo de medición, comprobación y presentación de este proyecto.

HERRAMIENTA SW	COSTE (€)
Windows 7 Professional	128,05
Wireshark	Libre
Microsoft Office 2010	380,79
PDF Creator	Libre
TOTAL	**508,84**

Tabla 1: Costes SW

Posteriormente, calcularemos el coste relativo a los recursos humanos. Si calculamos los recursos personales con la medida *hombre/mes,* obtenemos un valor que corresponde con el trabajo que una persona ha realizado durante 1 mes en 8 horas al día. Siendo equivalente a 4 semanas de 5 días de trabajo en cada una de ellas.

Tenemos en cuenta que una semana de trabajo corresponde con 5 días laborables (L-V). Durante los cuales una persona emplea 8 horas en cada uno de esos días.

Para este proyecto hemos contado con una ingeniera proyectista cuyas retribuciones se muestran en la tabla siguiente.

RECURSO HUMANO	CATEGORÍA	DEDICACION HORAS	COSTE HORA(€)
Sara Muñoz Hurtado	Ingeniera Junior *	640	40
TOTAL			**25600**

Tabla 2: Costes Recursos Humanos

* Corresponde con la labor de la ingeniera proyectista, cuyo coste por hora se establece en 40€/hora

A continuación se muestra el coste de los recursos materiales empleados necesarios para el desarrollo del proyecto. Para llevar a cabo este cálculo teniendo en cuenta la depreciación de los equipos, hemos empleado la siguiente fórmula:

TOTAL (€) = (MESES_DED/PERIODO_DEP)*PRECIO_UNIT*DED (%))

RECURSO MATERIAL LABORAL	CANTIDAD	PRECIO UNITARIO (€)	DEDICADO	MESES DEDICACION	PERIODO DEPRECIACION	TOTAL(€)
Ordenador Portátil	1	799	100%	4	60	53,27
Equipo NAT completo**	1	50000	50%	2	60	833,33
Dongle 3G	1	40	50%	2	60	0,67
TOTAL						887,27

Tabla 3: Costes Recursos Material

** Incluimos todas las funcionalidades que se han integrado en la plataforma a pesar de que para este proyecto, todos los módulos no sean lo suficientemente relevantes.

En este apartado incluimos aquellos gastos que el proyecto haya podido acarrear, y que no tienen por qué estar vinculados al desarrollo del mismo. En este sentido se trata del consumo eléctrico, limpieza, agua… Debido a que la estimación de los mismos resulta una tarea complicada, suponemos una tasa del 20% sobre el resto de costes.

El coste final del proyecto se calculará realizando el cómputo de los costes de las herramientas de SW, recursos humanos, materiales y los costes indirectos

COSTES	TOTAL (€)
HERRAMIENTA SW	508,84
RECURSO HUMANO	25.600,00
RECURSO MATERIAL LABORAL	887,27
SUBTOTAL	26.996,11
INDIRECTOS (20%)	5.399,22
TOTAL	32.395,33

Tabla 4: Costes Totales

El coste total del desarrollo del proyecto computa un total de **32.395,33 € (treinta y dos mil trescientos noventa y cinco euros con treinta y tres céntimos de euro).**

Es importante destacar que este proyecto es sólo una parte de otro global desarrollado en operadora móvil que desea desarrollar una solución basada en NAT al problema de acceso a su red 3G, pues tanto la estimación del crecimiento de usuarios, del tráfico generado y el límite de direcciones IPv4 muestran que para no restringir el crecimiento de Internet, es necesario asignar direccionamiento IPv4 privado a los usuarios móviles aplicando NAT.

5.1 Tareas

Las fases que engloban tareas como diseño a bajo nivel, definición de configuración de la red a implementar, instalación física de equipos, cableado de los equipos, replanteo, configuración de pruebas de aceptación final previas a la puesta en producción del equipo, integración de los equipos… no están incluidas en el objeto de este proyecto. Sin embargo las fases dedicadas al diseño de la batería de pruebas para comprobar el correcto funcionamiento de la plataforma NATBOX se desarrollan concretamente.

Documentación: Estudiamos los protocolos para comprender el funcionamiento de las plataformas integrantes del proyecto. Recopilamos por lo tanto la información y adquirir los conocimientos previos para el desarrollo del proyecto.

Desarrollo: Definimos los criterios a cumplir por los equipos, así como el escenario de pruebas diseñado para examinar las funcionalidades requeridas. Incluimos también el desarrollo y el resultado de la ejecución de los ensayos específicos.

Conclusiones: Exponemos las conclusiones obtenidas tras evaluar los resultados obtenidos de las pruebas definidas. Asimismo analizamos los trabajos futuros que pueden desarrollarse tanto en arquitectura como en definición de políticas funcionales, incluso alguna problemática que ha podido surgir durante todas las fases.

Tareas	Duración horas	Duración semanas
Documentación	**160**	**4**
Evolución Redes Móviles	20	
Evolución Smartphones	20	
Estudio Protocolo Enrutamiento	60	
Aplication Layer Gateway	60	
Desarrollo	**320**	**8**
Evaluacion equipos	50	
Escenario Pruebas	120	
Pruebas Realizadas	150	
Conclusiones	**40**	**1**
Análisis resultados	30	
Trabajos futuros	10	
Escritura memoria	**120**	**3**

Tabla 5: Duración fases proyecto

Planificamos el proyecto en varias fases bien diferenciadas que se han desarrollado durante 16 semanas y cuyos costes se especifican a continuación:

A continuación presentamos el diagrama de Gantt con la duración de las tareas representadas a lo largo del tiempo, estableciendo la jornada laboral en 8 horas en una semana de cinco días (L-V).

Tareas	inicio	Duración dias	fin
Documentación	**02/09/2013**	**20**	**27/09/2013**
Evolución Redes Móviles	02/09/2013	2,50	04/09/2013
Evolución Smartphones	04/09/2013	2,50	06/09/2013
Estudio Protocolo Enrutamiento	09/09/2013	7,50	18/09/2013
Aplication Layer Gateway	18/09/2013	7,50	27/09/2013
Desarrollo	**30/09/2013**	**40**	**25/11/2013**
Evaluacion equipos	30/09/2013	6,25	08/10/2013
Escenario Pruebas	08/10/2013	15	29/10/2013
Pruebas Realizadas	29/10/2013	18,75	25/11/2013
Conclusiones	**26/11/2013**	**5**	**02/12/2013**
Análisis resultados	26/11/2013	3,75	29/11/2013
Trabajos futuros	29/11/2013	1,25	02/12/2013
Escritura memoria	**03/12/2013**	**15**	**24/12/2013**

Tabla 6: Diagrama de Gantt

Como podemos comprobar las tareas más importantes pertenecen al apartado de desarrollo.

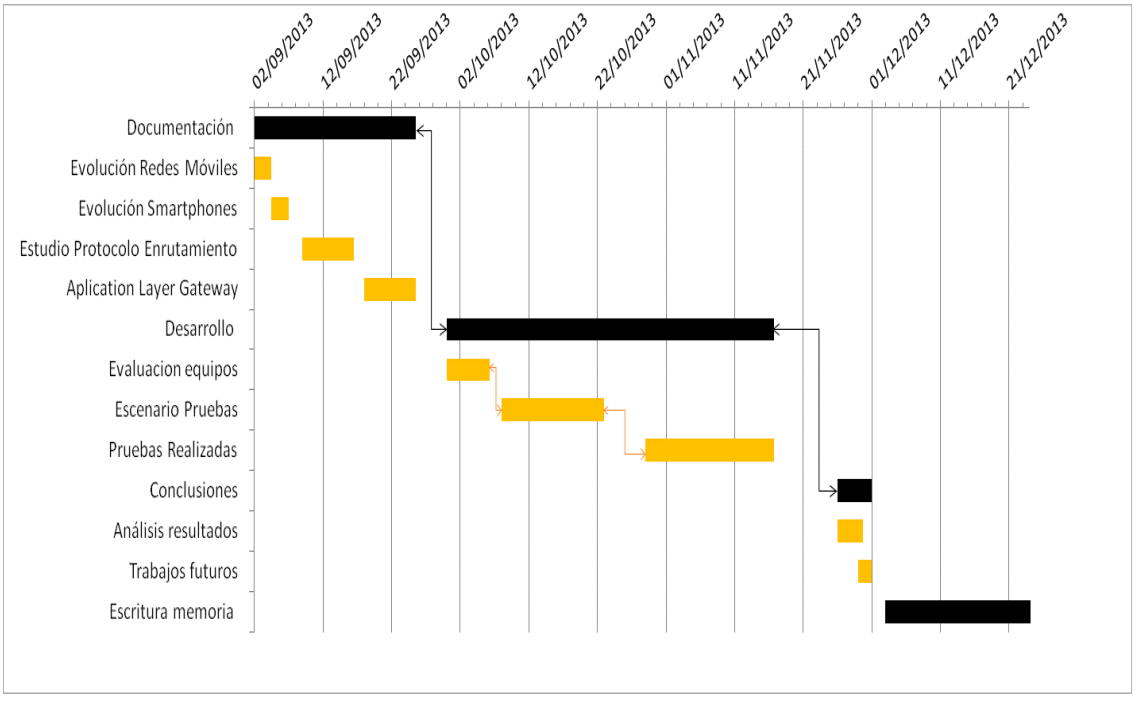


Tabla 7: Diagrama de Gantt

GLOSARIO

NAT: Network Access Translation

RFC: Requests for comments

DPC: Dense Port Concentrators (Chasis de Juniper)

BGP: Border Gateway Protocol

EBGP: External Border Gateway Protocol

ALGs: Application Level Gateway

VoIP: Voice over Internet Protocol

P2P: Peer to Peer

IPSec: Internet Protocol Security

IPS: Intrusion Prevent System

OSPF: Open shortest path first

GGSN: Gateway GPRS Support Node

APN: Access Point Name

FTP: File Transfer Protocol

H.323: Parte de los protocolos H.32X

SIP: Session Initiation Protocol

RSTP: Rapid Spanning Tree Protocol

ICMP: Internet Control Message Protocol

TFTP: Trivial file transfer Protocol

DNS: Domain Name System

IRC: Internet Relay Chat

PPTP: Point to Point Tunneling Protocol

DCCP: Datagram Congestion Control Protocol

GRE: Generic Routing Encapsulation

SCTP: Stream Control Transmission Protocol

Gi: Gateway Initiated

UMTS: Universal Mobile Telecommunications System

3GPP: 3rd Generation Partnership Project

LTE: Long Term Evolution

QoS: Quality of Service

UMTS: Universal Mobile telecommunications System

UTRAN: Terrestrial Radio Access Network

ENB: envolved Node B

IMS: Internet Protocol Multimedia Subsystem

RIPE: Réseaux IP Européens (Centro de coordinación de redes IP Europeas)

ISP: Internet Services Providers

RIRS: Regional Internet Registries, Registros Regionales de internet

IANA: Internet Assigned Numbers Authority

AG: Access Gateway. A gateway in the access network

HA: Home Agent

NAT44: Network Address Translation IPv4 to Ipv4

PDN- GW: Packet Data Network

CGN: Carrier Grade NAT

HTTP: Hypertext Transfer Protocol

URL: Uniform resource locator

POP3: Post Office Protocol 3

SSL: Secure Socket Layer

Smartphones: es un teléfono móvil basado en un sistema operativo para móviles, con mayor conectividad y capacidad que un teléfono corriente.

Roaming: término general que se refiere a la posibilidad de emplear el servicio de conectividad en una ubicación distinta del proveedor donde se registró el mismo servicio.

TMA: Telefonía Móvil Automática

MS: Mobile Station

BTS: Base Transceiver Station

GSM: Global System for Mobile communications

RDSI: Red Digital Servicios Integrados

SMS: Short Message Service

BSC: Base Station Controller

BSS: Base Station System

MSC: Mobile System Controller

SGSN: Serving Gateway Support Node

VLR: Virtual Location Register

HLR: Home Location Register

EDGE: Enhanced Data Rates for GSM Evolution

ATM: Asynchronous Transfer Mode

UMTS: Universal Mobile Telecommunications System

UE: User Equipment

CN: Core Network

RNC: Radio Network Controller

LTE: Long Term Evolution

QoS: Quality of Service

ESP: Encapsulating Security Payload

ISAKMP: Internet Security Association and Key Management Protocol

SSDP: Simple Service Discovery Protocol

BIBLIOGRAFIA

[1] Arquitectura Red Móvil GSM. Jose Manuel H. Moya *Comunicaciones Móviles. Sistemas GSM, UMTS y LTE.* Ra-Ma, España ,2012.

[2] Arquitectura Red Móvil GPRS. Regis J. Bates *General Packet Radio Service.* McGraw-Hill, New York, 2002.

[3] Arquitecturas Tecnología UMTS y Tecnología UTRAN. Kaaranen Heikki. *Redes UMTS. Arquitectura, movilidad y servicios.* Alfaomega, España, 2006.

[4] Arquitectura Red Long Term Evolution: LTE http://www.4gamericas.org/documents/3GPP_Rel-8_Beyond_02_12_09

[5] Ranking Países uso de smartphones, [6] Porcentaje usuarios always on según el acceso, [7] Distribución tipo de dispositivos de acceso a la red http://www.fundacion.telefonica.com/es/que_hacemos/noticias/detalle/10_01_2013_esp_2430

[8] Modelo de Referencia OSI. *The ISO Model of Architecture for Open Systems Interconnection.* Hubert Zimmermann, *IEEE Transactions on Communications*, vol.28, no. 4, April 1980, pp 425-432.

[9] Asignación direccionamiento IP http://www.nro.net/

[10] Internet Protocol http://tools.ietf.org/html/rfc791

[11] Address Allocation for Private Internets http://tools.ietf.org/html/rfc1597

[12] IP Networks Address Translator (NAT) Terminology and Considerations http://tools.ietf.org/html/rfc2663

[13] Network Address Translation (NAT) Behavioral Requirements for Unicast UDP http://tools.ietf.org/search/rfc4787

[14] An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition http://tools.ietf.org/html/rfc6264

[15] Nat 46 Considerations http://www.ietf.org/proceedings/77/slides/behave-9.

[16] DNS64 Extensions for Network Address Translation http://tools.ietf.org/search/rfc6147

[17] Gateway-Initiated Dual-Stack Lite Deployment http://tools.ietf.org/html/rfc6674

[18] Hypertext Transfer Protocol http://www.ietf.org/rfc/rfc2616.txt

[19] Transmission Control Protocol http://tools.ietf.org/search/rfc793

[20] Internet Message Access Protocol http://tools.ietf.org/html/rfc3501

[21] Post Office Protocol http://www.ietf.org/rfc/rfc1939.txt

[22] The Secure Sockets Layer (SSL) http://tools.ietf.org/html/rfc6101

[23] Security Architecture for the Internet Protocol http://tools.ietf.org/search/rfc4301

[24] Documentación Técnica Equipos del fabricante correspondiente.

[25] Herramienta Wireshark

[26] Internet Security Association and Key Management Protocol http://www.ietf.org/rfc/rfc2408.txt